ADD-ONS
für Mozilla Firefox

Der Open-Source-Webbrowser Firefox (`www.mozilla-europe.org/de/firefox/`) erfreut sich nicht zuletzt auf Grund seiner einfachen Erweiterbarkeit mittels freier Add-ons immer größerer Beliebtheit. Dabei ist es unmöglich, alle Add-ons zu kennen, geschweige denn selber auszuprobieren. Selbst bei gezielter Suche kann es schwer fallen, das Passende zu finden. An dieser Stelle – und auch in zukünftigen Ausgaben des comment – möchten wir Ihnen aus der Fülle an erhältlichen Erweiterungen einige besonders brauchbare Gustostücke vorstellen.

Was ist ein Add-on?

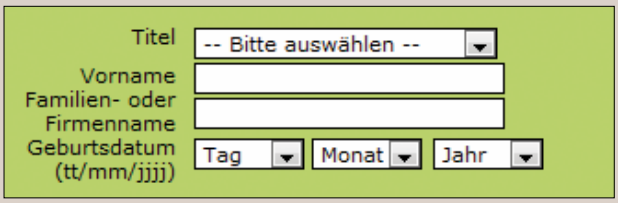
Ein Add-on (engl. to add = hinzufügen) bezeichnet ein optionales Modul, welches bestehende Software um eine Funktionalität ergänzt oder erweitert. Bekannt sind Add-ons vor allem als Erweiterung eines Webbrowser, die man ganz nach Belieben installieren und somit den Browser persönlichen Bedürfnissen anpassen kann.

Add-ons sollten nur von vertrauenswürdigen Quellen bezogen werden, dazu zählt die offizielle Webseite von Mozilla `https://addons.mozilla.org/de/firefox`. Der Großteil der hier verzeichneten Add-ons – derzeit über 5.000 – ist kostenlos.

Text Area Resizer & Mover

Haben Sie sich auch schon des Öfteren beim Ausfüllen von diversen Webmasken oder Onlineformularen über viel zu kleine Eingabefelder geärgert? Der Designer hat dann oft nicht bedacht, dem Namen Maximilian Mustermann genügend Raum in einem Ausfüllfeld zu spendieren. Dadurch kann es passieren, dass Teile der Eingabe verdeckt werden, wodurch es leicht zu Tippfehlern kommt. Hier kann das Add-on *Text Area Resizer & Mover* helfen. Es ermöglicht auf einfachste Weise eine **Vergrößerung bzw. das Verschieben eines Eingabefeldes auf Webseiten**.

Onlineformular, bei dem die Eingabefelder zu klein bzw. auch unübersichtlich angeordnet sind.



Mit dem Text Area Resize & Mover lassen sich diese Felder in der Größe anpassen und an andere Stellen verschieben.

Der Text Area Resizer kann unter `https://addons.mozilla.org/de/firefox/addon/8287` heruntergeladen werden. Nach der vollautomatischen Installation und anschließendem Neustart des Browsers ist das Add-on aktiv. Nun lassen sich sämtliche Eingabefelder mittels Rechtsklick und gleichzeitigem horizontalen Ziehen mit der Maus in ihrer Breite anpassen.

Zusätzlich ist eine Verschiebung jedes Textfelder möglich. Mittels Rechtsklick in ein Feld öffnet sich das Kontextmenü, in dem bei installiertem Add-on der Eintrag *Enable element moveability* zu finden ist. Wählen Sie diese Option einmalig aus. Damit können zukünftig alle Eingabefelder mit Klick und gehaltener rechter Maustaste beliebig im Browserfenster verschoben werden. Dieses Feature kann auf gleichem Wege auch wieder deaktiviert werden, indem der Eintrag *Disable element moveability* aus dem Kontextmenü gewählt wird.

Eine Einschränkung gibt es allerdings: Die Größenänderung funktioniert leider nicht bei allen Formularelementen. Bei Upload-Feldern, Radio- und Checkboxen ist nur Verschieben möglich. Eine Ausnahme bilden auch mehrzeilige Textfelder. Diese sind auch vertikal maximierbar. Zudem bleibt die veränderte Größe bei allen Elementen nur für den aktuellen Besuch bestehen. Bei neuerlichem Aufruf der Seite erscheint wieder das originale Ausmaß.

Weitere Einstellungen lassen sich wie bei allen Add-ons in Firefox unter *Extras – Add-ons – Text Area Resizer and Mover – Einstellungen* vornehmen.

Alexander Berndl

IPv6-Tunnel im Uni-Datennetz

Worauf InternetnutzerInnen derzeit noch achten müssen

Foto: sxc.hu

Was ist IPv6?

Das **Netzwerkprotokoll** IPv6 ist der Nachfolger des derzeit noch überwiegend verwendeten Internetprotokolls der Version 4 (IPv4). Dieses ist die **Grundlage des Internet**, auf dessen Basis es möglich wird, Computer in größeren Netzwerken zu adressieren und Verbindungen zu ihnen aufzubauen. IPv6 wird bereits von zahlreichen Betriebssystemen sowie Endanwendungen unterstützt. Beide Versionen können ohne Probleme gleichzeitig betrieben werden.

IPv4 bietet einen Adressraum von 4,3 Milliarden **IP-Adressen** (2^{32} = 4.294.967.296)[1], mit denen Computer und andere Geräte angesprochen werden können. In den Anfangstagen des Internet, als es nur wenige Rechner gab, die eine IP-Adresse benötigten, galt dies als weit mehr als ausreichend. Aufgrund des Wachstums des Internet herrscht heute jedoch **Adressenknappheit**. Schätzungen zufolge könnten bereits 2011 die letzten IPv4-Netze vergeben und ein Jahr später keine weiteren Adressen mehr bereitgestellt werden. Durch IPv6 vergrößert sich der Adressraum auf 2^{128}, in Worten sind das 340 Sextillionen Adressen. Eine Sextillion sind die Ziffer 1 gefolgt von 36 Nullen:

1.000.000.000.000.000.000.000.000.000.000.000.000

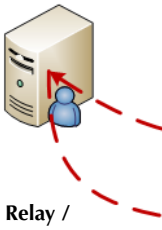
Der neue IPv6-Standard gewinnt also aufgrund der begrenzten Anzahl noch verfügbarer IPv4-Adressen an Bedeutung. Aktuelle Betriebssysteme wie Windows 7 oder MAC OS X 10.6 haben IPv6 in der Standardkonfiguration bereits aktiviert. In Windows werden zudem für den Umstieg von IPv4 auf IPv6 so genannte **Tunnelschnittstellen** automatisch eingerichtet, die der **Kommunikation von IPv4- mit IPv6-Endgeräten** dienen (siehe Abbildung).

Hinweis

Um Probleme zu vermeiden, sollte die Freigabe einer Netzwerkverbindung im Datennetz der Universität Wien immer abgeschaltet werden.

Eine Anleitung für Windows Vista/7 und Mac OS 10.6 finden Sie auf den ZID-Webseiten unter: `www.univie.ac.at/ZID/anleitungen-sonstiges/ipv6/`.

Wahrscheinlich jeder, der das Datennetz der Universität Wien nutzt, ist bereits – wenn auch unwissentlich – mit IPv6 (*Internet Protocol Version 6*) in Berührung gekommen. Ohne dessen Vorläufer, dem Internetprotokoll der Version 4 (IPv4), würde es das Internet, wie wir es heutzutage nutzen, überhaupt nicht geben (siehe Kasten: *Was ist IPv6?*).



6to4 Relay / IPv6 Tunnel Broker

Ob IPv4 oder IPv6, für die meisten NutzerInnen ist das im Grunde völlig unerheblich, da Netzwerke und Endgeräte die Modalitäten deren Verwendung selber regeln und EndanwenderInnen davon gewöhnlich nichts bemerken sollten.

IPv6-Tunnel im Uni-Datennetz

Im Datennetz der Universität Wien kann es derzeit jedoch vereinzelt zu **Verbindungsproblemen mit den E-Mail- und Webservern** der Universität kommen. Ursache des Problems ist eine aktivierte Funktion im Betriebssystem zur **Freigabe einer Netzwerkverbindung**, auch *Internet Connection Sharing* (ICS) genannt (siehe Kasten: *Internet Connection Sharing*).

In einem IPv6-Netzwerk, wie das Datennetz der Universität Wien, senden alle Router[2] in regelmäßigen Abständen spezielle „Nachrichten“ (*Router Advertisements*)[3] an alle Endgeräte, um diesen relevante Daten und Adressen des Netzwerks mitzuteilen. Im Normalfall verwenden alle an das Datennetz und WLAN der Universität Wien angeschlossenen Computer die Router Advertisements mit der höchsten Präferenz, also jene, die von den Routern der Universität verteilt werden. Durch aktiviertes Internet Connection Sharing werden jedoch **zusätzliche IPv6-Tunnelverbindungen** für andere Endgeräte freigegeben, die ebenfalls über Router Advertisements angekündigt werden.

Eine Kombination aus Internet Connection Sharing, einer Firewall, die IPv6- Router Advertisements blockt und/oder eines reinen IPv4-Netzwerks kann dazu führen, dass ein Endgerät im Datennetz der Universität Wien diese zusätzlichen, nicht funktionsfähigen bzw. gesperrten IPv6-Tunnel für andere Endgeräte ankündigt und damit einen Verbindungsaufbau zu Geräten mit IPv6-Adressen, im diesem Falle `www.univie.ac.at` verhindert (dargestellt in der Grafik). Im Datennetz der Universität Wien kann Internet Connection Sharing zu einem **Sicherheitsproblem** werden, wenn freigegebene Tunnelverbindungen anderen Rechnern im Netzwerk zur Verfügung stehen, weshalb **Tunnelverbindungen im Datennetz der Universität Wien aus Sicherheitsgründen gesperrt** werden.

1) Tatsächlich sind es weniger, da viele Adressen für interne Zwecke verwendet werden.

2) Router (auch: Gateway): Netzwerkgerät, das für die Weiterleitung von Datenpaketen im Netzwerk verantwortlich ist.

3) Router Advertisement: Datenpakete, die von einem Router verschickt werden, um den Endgeräten ihre Netzwerkkonfiguration mitzuteilen.

Mehr über IPv6 im comment

IPv6 im Uni-Datennetz
`http://comment.univie.ac.at/05-1/31/`

IPv6 – Das Internetprotokoll der nächsten Generation
`http://comment.univie.ac.at/03-1/35/`

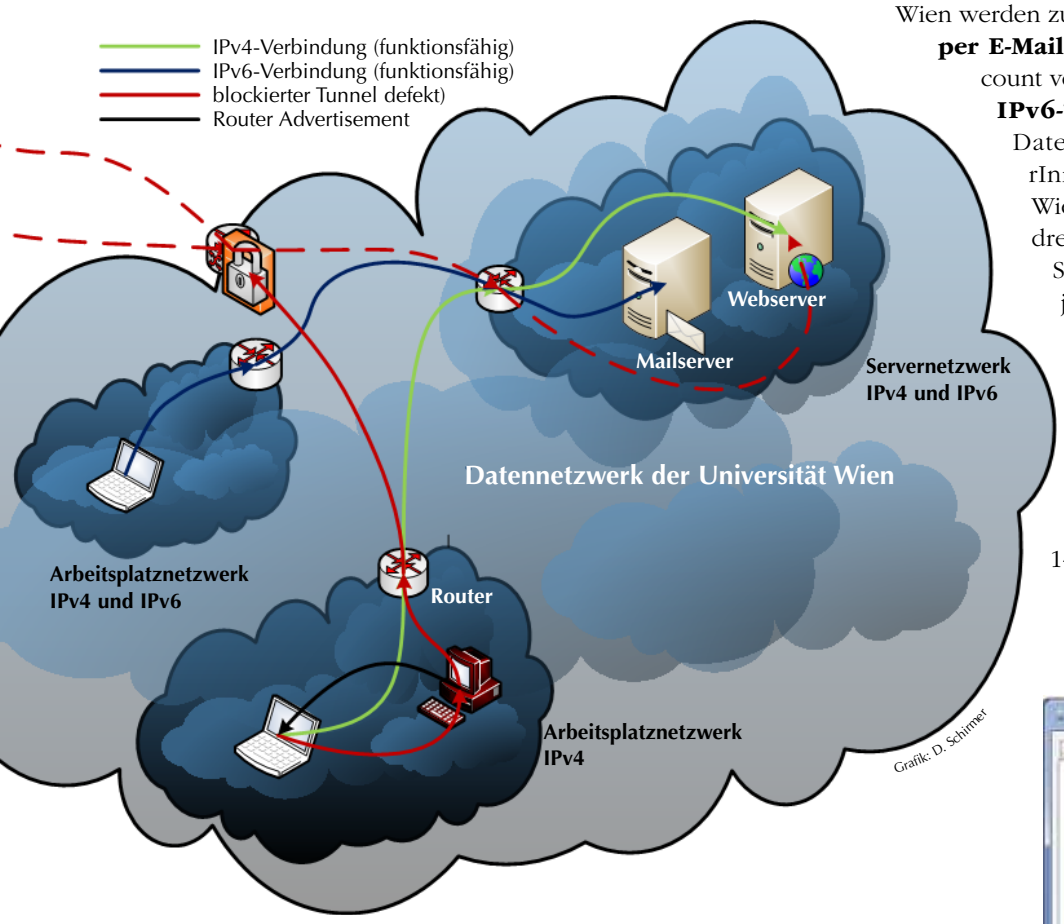
Information & Hilfe

Sollten Sie innerhalb des Uni-Datennetzes Probleme beim Zugriff auf die E-Mail- bzw. Webserver der Universität Wien haben, kontaktieren Sie bitte Ihre/n **EDV-BetreuerIn** bzw. kontrollieren Sie Ihre Einstellungen zur Internetverbindungsfreigabe (Anleitung siehe `www.univie.ac.at/ZID/anleitungen-sonstiges/ipv6/`).

BenutzerInnen des Kabel- oder Funkdatennetzes (Institutsnetze, u:connect und eduroam) der Universität Wien werden zudem vom Zentralen Informatikdienst **per E-Mail** über ihren Mailbox- oder u:net-Account verständigt, **wenn eines ihrer Geräte IPv6-Tunnel ankündigen** sollte. Falls Datenverbindungen anderer BenutzerInnen oder Services der Universität Wien dadurch gestört werden, ist nach dreimaliger E-Mail-Warnung auch eine Sperre des Netzwerkzugangs für den jeweiligen Computer/das jeweilige Notebook möglich.

Fragen zu IPv4/IPv6-Einstellungen im Datennetz der Universität Wien beantwortet auch der **Helpdesk des ZID** (`helpdesk.zid@univie.ac.at`), telefonisch unter 01-4277 140 60 von Mo – Fr 9 – 18 Uhr.

Daniel Schirmer

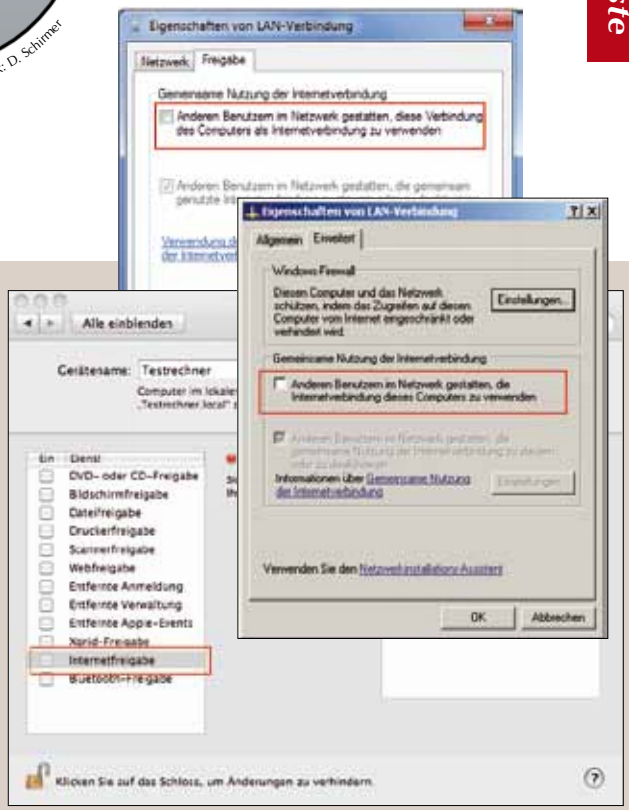


Internet Connection Sharing

Als **Internetverbindungsfreigabe** (*Internet Connection Sharing, ICS*) bezeichnet man eine Funktionalität von Betriebssystemen, die es ohne größeren technischen Aufwand und zusätzlicher Netzwerkgeräte ermöglicht, **den Internetzugang eines Computers auch anderen Geräten zur Verfügung** zu stellen, z. B. kann beim Anschluss einer Spielekonsole dieser automatisch der Zugang ins Netz ermöglicht werden. Dafür wird eine so genannte **Tunnelverbindung** errichtet, auch ohne dass dies der User bemerkt.

Dabei stellt der Computer, der ICS aktiviert hat, die Dienste NAT (*Network Address Translation*), DHCP-Server (*Dynamic Host Configuration Protocol*) und DNS-Server (*Domain Name Service*) zur Verfügung. Somit ist es möglich, dass weitere Geräte, die per LAN oder WLAN direkt an den freigebenden Computer oder Laptop angeschlossen sind, dessen Internetanbindung nutzen können, ohne dass weitere Dienste oder Server vorhanden sein müssen.

Die Bezeichnung Internet Connection Sharing stammt ursprünglich von Windows, welches diese Funktion seit Windows 98 SE anbietet. Unter Mac OSX wird dieses Feature als **Internetfreigabe** bezeichnet.



Internetverbindungsfreigabe in Windows Vista/7, Windows XP und Mac OS 10.6; Anleitung unter: www.univie.ac.at/ZID/anleitungen-sonstiges/ipv6/

Foto: sxc.hu

Handy entlaufen

Was nun?

Ob aus eigener Erfahrung oder durch Erzählung von Bekannten, fast jeder kennt die Situation: Das Mobiltelefon ist – vielleicht sogar durch „Fremdeinwirkung“ – abhanden gekommen. Dennoch ist vielen kaum bewusst, was einen zusätzlich zum Verlust des Gerätes erwarten kann bzw. welche vorbeugenden Maßnahmen man für den Fall des Handyverlustes treffen sollte. Mit ein wenig Wissen kann nämlich verhindert werden, dass sich zum vorübergehenden Verzicht auf die gewohnte ständige Erreichbarkeit noch weit schmerzlichere Erfahrungen gesellen.

Den Teufel an die Wand gemalt

Finanzieller Verlust

Wie könnte die Schadensbilanz im schlimmsten Fall aussehen? Zunächst einmal ist das wohldesignte Gerät samt Zubehör wie dem modischen Case und dem eben erst nachgekauften Akku weg. Der Preis für die Neuanschaffung kann dabei zwischen null und – wenn der laufende Vertrag noch keinen subventionierten Kauf erlaubt – mehreren hundert Euro liegen. Außerdem wird eine neue SIM-Karte (*Subscriber Identity Module*) fällig. Die Kosten dafür liegen bei üblichen Providerverträgen bei 10 bis 20 Euro.

Apropos SIM: Wussten Sie, dass dies sozusagen die Kreditkarte Ihres Mobiltelefons ist? Was bei der Kreditkarte die Kartennummer und das Ablaufdatum sind, ist beim SIM die sogenannte IMSI (*International Mobile Subscriber Identity*), über die die genutzten Dienste abgerechnet werden.[1)] Zwischen Kreditkarte und SIM-Karte besteht jedoch ein entscheidender Unterschied: Wenn man nämlich den Diebstahl oder Verlust nicht gleich bemerkt, haftet man bei der Kreditkarte nur für maximal 150 Euro[2)]. Bei der SIM-Karte hingegen muss man alle Gebühren, die vor der Sperre anfallen, in voller Höhe bezahlen! Das steht auch ganz deutlich in den AGB der Provider.

Kriminelle Banden könnten sich ein Körberlgeld verschaffen, indem sie mit gestohlenen Mobiltelefonen von ihnen selbst betriebene, kostenpflichtige Hotlines anrufen oder diverse Mehrwertdienste[3)] nutzen. Die dabei anfallenden Gebühren können richtig heftig werden: In Einzelfällen wurde über Rechnungen von mehreren tausend Euro berichtet![4)] Die gute Nachricht: Bislang ist die Professionalisierung in diesem Sektor offenbar noch nicht weit fortgeschritten und die drastischen Fälle bleiben noch die Ausnahme. Bei den wenigen gestohlenen Diensthandys der Universität Wien blieben die vertelefonierten Beträge bisher im zweistelligen Bereich.

Je mehr Dienste Sie mit Ihrem Handy nutzen, desto mehr Probleme kommen hinzu. Dazu nur zwei Beispiele: Haben Sie Paybox eingerichtet? Die Haftung beträgt je nach Nutzungsart zwischen 150 oder 750 Euro.[5)] Wird z. B. eine Tasche mit Telefon und Bankomatkarte gestohlen und steht im Telefonbuch unter dem Eintrag *Bankomat* eine vierstellige Zahl, braucht ein Dieb kein Einstein zu sein, um das Konto zu plündern.

Oft als „Handy ohne Vertrag“ fehlbezeichnet[6)], ist auch bei Wertkarten das Risiko nicht immer mit dem aufgeladenen Guthaben begrenzt. Das liegt daran, dass je nach technischer Umsetzung – also je nach Provider – manche Dienste verspätet abgerechnet werden können: Telefonate aus dem Ausland, im Ausland angerufen werden, Mehrwertdienste wie Klingeltonabonnements usw. Es ist also auch bei Prepaid-Verträgen durchaus möglich, dass Forderungen weit über das aufgeladene Guthaben hinaus entstehen und auch eingefordert werden.[7)]

Datenverlust

Zum direkt materiellen Schaden kommt noch, dass die am Handy gespeicherten Daten – Telefonnummern, Kalendereinträge, SMS-Nachrichten, Bilder, Musik etc. – weg sind, und zwar gleich in zweierlei Hinsicht. Erstens kann der/die berechtigte Benutzer/Benutzerin nicht mehr darauf zugreifen, was sich z. B. durch geplatzte Termine und verlorene Klingeltöne wieder in finanziellem Schaden äußern kann. Zweitens kann jetzt jemand anderer diese Daten lesen. Glücklicherweise mangelt es den meisten Kriminellen an Kreativität und Fähigkeit zu planmäßigem Handeln – aber oft lassen sich die gespeicherten Informationen gewinnbringend nutzen.

Es wurden auch schon bekannte Personen erpresst, die sehr private und nicht für die Öffentlichkeit bestimmte Bildchen am Telefon gespeichert hatten.[8)] Merke: In den Speicher des Mobiltelefons gehören keine Heimlichkeiten und keine Peinlichkeiten! Zu guter Letzt: Nicht auszudenken, welche Scherereien auf Sie zukommen, wenn das Telefon für kriminelle Handlungen missbraucht wird!

Schadensbegrenzung

Für ein paar Euro im Monat kann man sein Mobiltelefon versichern. Üblicherweise decken diese Versicherungen aber keine Gesprächsgebühren, sondern nur den Wert des Geräts – und das nicht einmal bei einfachem Verlust. Bei stark subventionierten Vertragsgeräten wird sich eine Versicherung also kaum auszahlen, allenfalls bei teuren Endgeräten, zumal die Versicherung auch Schäden durch Feuchtigkeit, Herunterfallen und ähnliches deckt.

Mehrwertdienste sperren

Eine wirksame Maßnahme zur Kostenvermeidung besteht darin, Nummernbereiche von teuren Mehrwertdiensten[9] zu sperren, wobei man wählen kann, ob das für Sprachtelefonie, SMS oder beide Dienste gelten soll. Das Sperren dieser Nummern kann je nach Provider bis zu 20 Euro kosten. Erkundigen Sie sich über Gebühren und Modalitäten der Sperre beim Kundenservice Ihres Providers! **Das Sperren von Mehrwertdiensten bei Diensthandys der Universität Wien ist kostenlos.** Senden Sie bitte eine E-Mail an handy.zid@univie.ac.at und geben Sie bitte genau an, ob Sie Sprache, SMS oder beide Dienste gesperrt bekommen möchten.

SIM-Karte mit PIN

Wie viele andere Chipkarten auch haben die in das Mobiltelefon eingesetzten SIM-Karten[10] den bekannten Zugriffsschutz mittels Geheimzahl, die als PIN (*Personal Identification Number*) bekannt ist, in den Mobiltelefonstandards aber eigentlich CHV (*Card Holder Verification Information*) genannt wird.Diese muss beim Einschalten des Mobiltelefons eingegeben werden, andernfalls verweigert die SIM-Karte die Zusammenarbeit, insbesondere die zum Einbuchen in das Mobilfunknetz notwendige Authentifizierung.

Um das Knacken der PIN mittels Durchprobieren zu verhindern, sperrt sich die Karte nach drei Fehlversuchen selbst und kann nur mittels *Personal Unblocking Key* (PUK) wieder freigeschaltet werden. Die Sicherung von Chipkarten mittels PIN und PUK ist an sich bekannt und bewährt. Dass sich die Karte selbst schützt und sich nicht auf das Handy verlässt, verhindert auch, dass etwa ein Dieb/eine Diebin sie einfach in ein anderes Gerät einsetzt und damit nach Herzenslust telefoniert.

Tastensperre mit Code? Ja bitte!

Gelangt ein Telefon in fremde Hände und ist es, wie wohl meistens in so einer Situation, bereits eingeschaltet, greift der PIN-Schutz der SIM-Karte nicht: Die PIN wurde ja bereits eingegeben und die SIM-Karte damit entsperrt. In dieser Situation muss das Telefon selbst den Missbrauch verhindern, und dafür gibt es bei vielen Modellen eine einfache Lösung: Die sich selbst aktivierende Tastensperre mit Sicherheitscode.

Wenn eine bestimmte Zeit lang keine Tasten gedrückt wurden, blockiert eine Tastensperre alle Funktionen des Telefons. Ist zusätzlich noch der Sicherheitscode aktiviert, werden die Tasten erst freigegeben, nachdem man einen geheimen Code eingegeben hat – mit der nützlichen Ausnahme, dass eingehende Anrufe weiterhin wie gewohnt entgegen genommen werden können.[11]

Im Kasten *Einstellen der Tastensperre mit Code am Beispiel des Nokia 2630* auf Seite 29 wird erklärt, wie sich bei vielen Nokia-Modellen diese Funktion aktivieren lässt. Leider verfügt nicht jedes Handy über eine Tastensperre mit Code, und werksseitig aktiviert ist sie schon gar nicht.

Mitunter lässt sich diese Funktion jedoch mit Software von Drittanbietern nachrüsten.[12]

Foto: sxc.hu

1) So wie auf Ihrer Kreditkarte nicht die Nummer Ihre Girokontos steht, speichert nicht die SIM-Karte Ihre Telefonnummer(n), sondern der Provider in einer Datenbank. Dadurch ist es z. B. möglich, ohne SIM-Tausch Rufnummern zu ändern, hinzuzufügen etc. bzw. umgekehrt die Rufnummer zu behalten, auch wenn die SIM-Karte verloren geht oder defekt wird.

2) Das ist zumindest bei den hierzulande üblichen Karten Visa und Mastercard der Fall. Mehr dazu unter https://www.kreditkarte.at/web/content/de/Notfall/Notfall_Kreditkarte/Kartensperre/index.html

3) Vgl. das Kapitel „Mehrwertdienste“ der Broschüre „Informations- und Kommunikationstechnologien (IKT) im Alltag: Auswirkungen auf Individuum und Gesellschaft“, online unter: www.rtr.at/de/komp/SchriftenreiheNr32007

4) In Extremfällen erreichen die Gebühren horrende Höhen, etwa $16,388 und $26,000 in www.turn.org/article.php?id=572 oder & 8000 in www.theregister.co.uk/2004/01/09/tmobile_waives/

5) Die höhere Grenze von EURO 750,- gilt, wenn der Missbrauch mit PIN-Eingabe erfolgt. Details stehen in den AGB unter Punkt 13.3 und 13.4, online unter www.paybox.at/287.php

6) In einer übereinstimmenden Willenserklärung verpflichten sich der Netzbetreiber zu einer Leistung, der Kunde zur Zahlung eines fixen Betrags, dabei gelten festgelegte Regeln – das ist ein ganz typischer Vertrag nach § 863 ABGB.

7) Das wurde u.a. im c‘t-TV am 7. Februar 2009 unter dem Titel *„Kostenfalle Kostenkontrolle“* deutlich erklärt. Online abrufbar unter: www.heise.de/ct-tv/video/Das-c-t-magazin-im-Fernsehen-393689.html

8) siehe www.sueddeutsche.de/panorama/550/463162/text/

9) Von dieser Sperre sind nur 09xx-Nummern erfasst, die bis zu EUR 3,64 oder EUR 10,00 pro Anruf/Event kosten dürfen. Dienste unter 118xx (Auskunft) und 08xx bleiben weiterhin erreichbar. Die genauen Tarife sind für Österreich in der Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 – KEM-V 2009 geregelt, online unter www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2009_II_212. Laut Auskunft der Regulierungsbehörde RTR dürfen Provider den Kunden die für die jeweilige Fernzone angegebenen Tarife verrechnen, dürfen aber im Gegenzug ausländische Mehrwertdienste filtern.

10) Von den Abmessungen der kleineren Plugin-SIMs abgesehen spezifiziert GSM nur unwesentliche Abweichungen von SmartCards nach ISO 7816, siehe ETS 300 977 (GSM 11.11).

11) Auch der Bildschirmschoner am PC sollte so eingestellt sein, dass er verhindert, dass Vorübergehende während der Kaffeepause oder einer Besprechung in Mail und vertraulichen Dokumenten herumstöbern oder etwas verändern können.

12 Über praktische Erfahrungsberichte mit solcher Software würde sich der Autor freuen, bitte Mail an: at@univie.ac.at

Handy-Notfallkarte

Sobald Sie den Verlust Ihres Handys bemerken, sollten Sie sofort handeln. Hilfreich ist in dieser Situation, alle erforderlichen Daten zur **Sperrung des Gerätes** bei der Hand zu haben. Bei der Übernahme Ihres Diensthandys erhalten Sie eine Notfallkarte, auf der die Nummern Ihres Handys (intern & extern), die Modellbezeichnung, IMEI und SIM-Nummer sowie die Rufnummern zur Sperrung angegeben sind.

universität wien

Max Mustermann

Offiziell	0664-60277 xxxxx
Intern	0664-xxxxxxx
Handy	z. B. Nokia 2630
IMEI	xxxxxxxxxxxxxxx
SIM	xxxxxxxxxxxxxx

Muster

Bei Verlust rufen Sie bitte umgehend bei A1 an und lassen Ihre Rufnummer sperren: 0800 664 602 oder 0800 664 664
Aus dem Ausland: +43 664 664 602 oder +43 664 664 664

Bei Verlust Ihres Diensthandys rufen Sie bitte umgehend eine der dort aufgeführten Nummern an und lassen Ihre interne Rufnummer sperren.

Schreiben Sie nach diesem Telefonat schnellstmöglich eine Verlustmeldung an `handy.zid@univie.ac.at`. Geben Sie dabei sowohl die offizielle als auch die interne Rufnummer des Handys an. Falls Sie eine der beiden Rufnummern nicht wissen, können Sie sich unter dem Link `https://www.univie.ac.at/ZID/handy-webmaske/` mit Ihrem Mailbox-Account einloggen und Ihre Rufnummer dort ablesen.

Falls das Gerät wieder gefunden wird, werden die Berechtigungen wieder aktiviert; anderenfalls muss ein Duplikat der SIM-Karte beantragt werden. Weitere Informationen dazu finden Sie unter `www.univie.ac.at/ZID/hardwarereplacement/`.

Die Tastensperre ist nicht Fort Knox: Spezialisten haben realistische Chancen, sie zu umgehen, aber ein Standarddieb wird mit einem mit Code gesicherten Gerät kaum etwas anfangen. Sollte der das Handy tatsächlich einem Fachkundigen zur weiteren Verwertung übergeben, haben Sie in der Zwischenzeit hoffentlich den Verlust bemerkt und die SIM-Karte gesperrt. Dieser Zeitgewinn kann bares Geld wert sein!

Haltet den Dieb!

Handyortung, Sperrlisten & Co: Die Chancen, ein gestohlenes oder unehrlich gefundenes Mobiltelefon wiederzuerhalten, stehen schlecht. Eine Hoffnung sei gleich zunichte gemacht: Die Ortung durch den Provider wäre nicht genau genug, um direkt in die Wohnung des Diebes zu führen. Obendrein wäre das administrative Prozedere zu aufwendig und die Kosten stünden in keinem tragbaren Verhältnis zum Wert des Geräts.

Wenn man dem Dieb/der Diebin doch wenigstens die Freude verderben könnte! Mobilfunknetze können Endgeräte anhand ihrer IMEI (*International Mobile Equipment Identity*, so etwas wie die Fahrgestellnummer beim Auto) aussperren. Damit das effektiv ist, müsste man weltweit bei jedem Provider einzeln diese Sperre beantragen. Die Realität ist ernüchternd: Eine IMEI-Sperre ist in Österreich nur bei Orange möglich[13], bei allen anderen Providern kann ein gesperrtes Telefon also ungehindert benutzt werden.

Es gibt zumindest einen plausiblen Grund, warum so viele Provider Sperrmuffel sind und warum nicht schon längst internationale Sperrlisten geführt werden: Die IMEI im Gerät kann man umprogrammieren. Mit sogenannten *Flashern*, die das Handy über die für Softwareupgrades vorgesehene Schnittstelle ansprechen, ist das bei den meisten Geräten relativ leicht möglich. Eigentlich logisch: Da die Systemsoftware dem Netz beim Einbuchen die IMEI bekanntgibt, kann eine als „Upgrade“ eingespielte, andere Software auch eine andere IMEI angeben.[14]

Übrigens: Wenn Sie ein gebrauchtes Telefon kaufen, können Sie die im Batteriefach angebrachte IMEI mit der im Display erscheinenden Nummer durch Eingabe von `*#06#` vergleichen. Stimmen sie nicht überein, handelt es sich wohl um Hehlerware.

Auch wenn die Aufklärungsquote gering ist, sollte man einen Diebstahl bei der Polizei anzeigen und dabei die IMEI des Gerätes angeben, damit diese in die sogenannte Sachfahndungsliste aufgenommen wird. Sollte das Telefon beispielsweise mit anderem Diebesgut irgendwo auftauchen, kann es dadurch dem/der rechtmäßigen Besitzer/Besitzerin zurückgegeben werden.

13) laut Auskunft der Pressestelle von Orange

14) Schlecht informierte, aber wohlmeinende Geister fordern gelegentlich, die IMEI müsse in einem unveränderbaren Speicher abgelegt werden. Über diese Idee können Techniker und Kriminelle nur müde lächeln: Manipulierte Software würde diese unveränderbare Nummer ganz einfach nicht auslesen, sondern eine andere verwenden.

15) Mangels praktischer Erfahrungen können wir keine konkreten Produkte empfehlen, freuen uns aber über Erfahrungsberichte an `at@univie.ac.at`

16) Einer Umfrage der Partnervermittlung Elitepartner zufolge haben 15% der Frauen und 10% der Männer bereits in den SMS ihrer Partnerin/ihres Partners gestöbert, abrufbar unter `www.elitepartner.de/presse/studien/LiebesTrendMonitor_2007.pdf`

„Anti-Diebstahl"-Software

Eine Handvoll Produkte verspricht[15], bestohlenen Handyeigentümern zu helfen. Der Funktionsumfang dieser „Anti-Diebstahl"-Software ist unterschiedlich, hat aber zwei Kernbereiche: Fernsteuern und Heimtelefonieren.

Zum einen lässt sich das Telefon über spezielle SMS-Nachrichten in gewissem Maße fernsteuern: Man kann Kontakte, Bilder oder gespeicherte Nachrichten löschen, das Gerät sperren oder über den Lautsprecher eine Alarmsirene ertönen lassen. Erfahrungsgemäß lassen Diebe das Telefon oft noch eine Zeit lang eingeschaltet, daher sind die Aussichten, damit noch etwas ausrichten zu können, gar nicht so gering.

Wechselt der Dieb die SIM-Karte, erkennt spezielle Software das und sendet eine SMS mit der neuen Telefonnummer und der Kennung der gerade aktiven Basisstation (quasi des nächstgelegenen Sendemasts) an eine zuvor festgelegte Nummer. Das soll die Ausforschung des Bösewichts ermöglichen, ob das in der Praxis funktioniert, mag bezweifelt werden. Man behält aber zumindest die Möglichkeit der Fernsteuerung.

Selbstverständlich funktioniert die Software nur solange sie nicht entfernt wird. Auch wenn sie sich noch so gut versteckt: Spätestens wenn die Firmware upgedatet wird, – hier kommt wieder der Flasher ins Spiel – ist auch die Software dahin.

Verwandte, Bekannte und sonstige Insider

Bisher sind wir von zwielichtigen, vor allem aber fremden Personen ausgegangen, die Handys entwenden. Als Täter kommen jedoch auch Bekannte oder Verwandte in Betracht: Sie können das Mobiltelefon an sich nehmen und später unbemerkt wieder zurückgeben. Die Gründe dafür können verschieden sein:

So ist es sicher keine Seltenheit, wenn Kinder mit dem Handy ihrer Eltern Unfug treiben – das Spektrum reicht hier vom Abrufen von Spielen und Klingeltönen über Anrufe bei Sexhotlines bis zu diversen Streichen.

Ein häufiger[16] und ernst zu nehmender Missbrauch im engen Familien- oder Bekanntenkreis ist das Herumschnüffeln in SMS und Anrufprotokollen des Partners/der Partnerin.

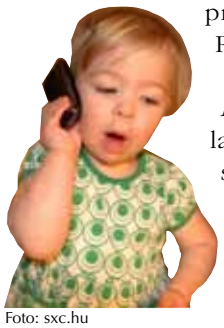


Foto: sxc.hu

Auch im Büro oder im Lokal lauern Gefahren: Hier könnte sich schnell jemand unbemerkt an einem herumliegenden Mobiltelefon zu schaffen machen. Dazu nur ein Beispiel:

Einstellen der Tastensperre mit Code am Beispiel des Nokia 2630

Foto: Nokia

1. Sicherheitscode wählen

Wählen Sie den Code, mit dem Sie hinkünftig Ihr Telefon entsperren. Dieser sollte mindestens fünf Ziffern lang und einigermaßen originell sein:

12345, 55555 oder Ihr Geburtsdatum wären eine weniger gute Wahl. Merken Sie sich den Sicherheitscode gut; wenn Sie ihn aufschreiben möchten, hinterlegen Sie ihn bitte an einem sicheren Ort (z. B. Tresor) und keinesfalls in der Schreibtischlade.

2. Sicherheitscode einstellen

Drücken Sie die Navigationstaste, um ins Menü zu gelangen. Wählen Sie dann *Einstellungen – Sicherheit – Zugriffscodes – Sicherheitscode ändern*. Geben Sie den alten Sicherheitscode ein – die Voreinstellung bei Nokia ist 12345 – und dann zwei Mal den von Ihnen gewählten Code. Bestätigen Sie jedes Mal die Eingabe mit der Navigationstaste. Danach drücken Sie die *Beenden*-Taste, um das Menü zu verlassen.

3. Optional: PIN einstellen

Wenn Sie möchten, können Sie die PIN der SIM-Karte auf den selben Wert wie den Sicherheitscode setzen. Dazu drücken Sie die Navigationstaste, um ins Menü zu gelangen. Wählen Sie dann *Einstellungen – Sicherheit – Zugriffscodes – PIN ändern*. Geben Sie die alte PIN ein und dann zwei Mal Ihren Sicherheitscode. Bestätigen Sie jedes Mal die Eingabe mit der Navigationstaste. Danach drücken Sie die *Beenden*-Taste, um das Menü zu verlassen.

4. Automatische Tastensperre aktivieren

Drücken Sie die Navigationstaste, um ins Menü zu gelangen. Wählen Sie dann *Einstellungen – Telefon – Automatische Tastensperre*. Bestätigen Sie die Einstellung *Ein*, dann stellen Sie die Zeit bis zur Aktivierung ein und bestätigen Sie mit der Navigationstaste. Drücken Sie die *Beenden*-Taste, um das Menü zu verlassen.

5. Sicherheits-Tastensperre aktivieren

Drücken Sie die Navigationstaste, um ins Menü zu gelangen. Wählen Sie dann *Einstellungen – Telefon – Sicherheits-Tastensperre*. Bestätigen Sie die Einstellung *Ein* drücken Sie die *Beenden*-Taste, um das Menü zu verlassen.

10 + 5 praktische Tipps

Im Vorfeld

1. Achten Sie bereits bei der Anschaffung darauf, dass das Gerät über eine **automatische Tastensperre mit Sicherheitscode** verfügt.
2. **Aktivieren** Sie die Tastensperre mit Sicherheitscode und deaktivieren Sie keinesfalls die Abfrage der PIN beim Einschalten des Geräts. Wählen Sie einen guten Code – nicht etwa 1234 oder 0000.
3. Kleben Sie eine **Kontakttelefonnummer in das Batteriefach** (bei Geräten, die über dieses verfügen). Das erhöht Ihre Chance, dass ein ehrlicher Finder das Gerät schnell retourniert.
4. Hinterlegen Sie die für die Sperre benötigten Daten, **Sperrnotrufnummer** und IMEI an sicherer Stelle, möglichst so, dass Sie auch auf Reisen darauf zugreifen können. Was Sie für eine Sperre benötigen, erfahren Sie auf der Homepage Ihres Providers, ür Diensthandys der Universität Wien informieren Sie sich bitte unter `www.univie.ac.at/ZID/handy-verlust/`.
5. Hinterlegen Sie auf gleiche Weise alle Informationen, die Sie benötigen, um **mit dem Mobiltelefon verbundene Services** wie z. B. PayBox zu sperren.
6. Notieren Sie die genaue **Modellbezeichnung**, Seriennummer, Farbe und Ausstattung Ihres Telefons.
7. Speichern Sie **keine vertraulichen Informationen auf dem Handy** und sorgen Sie regelmäßig für Backups der wichtigen Daten.
8. Lassen Sie **Dienste**, die Sie nicht benötigen, durch Ihren Provider **sperren** (z. B. Mehrwertrufnummern, Roaming, GPRS, MMS).
9. **Verwahren Sie Ihr Handy** ebenso **sorgfältig** wie Bargeld, z. B. in einer verschlossenen Gürteltasche.
10. Sollten Sie Ihr **Mobiltelefon** samt (Prepaid-)SIM-Karte **verkaufen**, melden Sie das bei Ihrem Provider.

Wenn es passiert ist

Sobald Sie bemerken, dass das Mobiltelefon abhanden gekommen ist, gilt es, rasch zu reagieren.

1. **Wenn Sie nicht ganz sicher sind, dass Sie es nicht bloß verlegt haben**: Rufen Sie es an und horchen Sie, ob Sie es läuten hören. Wenn Sie Bluetooth konfiguriert und eingeschaltet haben, können Sie auch bei einem lautlos gestellten Gerät feststellen, ob es sich in Ihrer Nähe befindet.
2. Lassen Sie die **SIM-Karte sofort sperren**.
3. Lassen Sie **zusätzliche Dienste**, z. B. PayBox, **sperren**.
4. Wenn das Telefon gestohlen wurde: Erstatten Sie **Anzeige bei der Polizei** und geben Sie die IMEI an.
5. Wenn das Telefon bei einem Wohnungseinbruch gestohlen wurde: Melden Sie den Schaden bei der **Haushaltsversicherung**.

Ein rivalisierender Kollege ruft bei Vorgesetzten oder Kunden an oder sendet ihnen eine SMS-Nachricht, deren Inhalt weniger dem guten Ton entspricht. Anhand der Rufnummer wird der nichtsahnende Handyeigentümer als Urheber identifiziert. Dieser wird zumindest einige Mühe haben, die Beleidigten davon zu überzeugen, dass nicht er, sondern der große Unbekannte sich einen Scherz erlaubt hat. Der Kollege könnte auch raffinierter und perfider vorgehen: Er könnte falsche Informationen verbreiten, deren Auswirkungen nicht sofort auffallen. Der Betroffene hätte kaum eine Chance zu erkennen, wie es zu den ihm zugerechneten Fehlleistungen gekommen ist und könnte sich auch nicht angemessen gegen die aufkommenden Vorwürfe verteidigen.

Das Handy wird gerade im E-Commerce gerne als vertrauenswürdiger Kanal zur Bestätigung von Transaktionen verwendet. Der Bezahldienst Paybox setzt ein Musterbeispiel einer Zwei-Faktor-Authentifizierung ein: Soll eine Zahlung getätigt werden, ruft Paybox das Mobiltelefon an: Nun muss der Besitzer/die Besitzerin den Auftrag durch Drücken auf *OK* oder Eingabe einer PIN freigeben. Diese Vorgangsweise geht davon aus, dass es kaum jemanden gelingen wird, sowohl die PIN auszuspähen, als auch das Gerät in Besitz zu bringen. Ein Insider kann aber einen Schwachpunkt ausnützen: Um von Paybox eine neue PIN zu erhalten[17], braucht man nur das Telefon und die Kenntnis einer Sicherheitsfrage, z. B.: *Wie hieß Ihr erstes Haustier?* Genau dies kann man als Bekannter aber völlig unverdächtig in einer Plauderei erfahren oder vielleicht sogar auf der Homepage nachlesen, dann die PIN neu setzen, nach Belieben shoppen und das Mobiltelefon wieder zurückgeben. Aus Sicherheitssicht können wir nur empfehlen, derartige (Un)Sicherheitsfragen nie wahrheitsgemäß zu beantworten, sondern als das zu behandeln, was sie sind: Als Passwort, und das darf nicht unsicherer sein, als die PIN, die es schützen soll.

Gegen all dies hilft die bereits empfohlene Tastensperre – Zugangscodes und Passwörter gehören übrigens auch im Familienkreis zur Privatsphäre.

Fazit

Im Mobiltelefon steckt nicht nur ein Haufen Hochtechnologie, sondern auch eine Menge Geld in verschiedenen Erscheinungsformen. Daher sollte man es nicht als ein Gerät der Unterhaltungselektronik[18] unterschätzen, sondern wie einen Wertgegenstand behandeln und alle zur Verfügung stehenden Sicherheitsvorkehrungen nutzen.

Alexander Talos-Zens

17) Laut Auskunft von Paybox

18) Der Unterhaltungswert für die Mitreisenden, die nach der für sie nicht informativen Einleitung „Ja, ich bin im 48A!“ lautstark mit allen möglichen intimen Details ihnen unbekannter Personen versorgt werden, bleibt allerdings fragwürdig.

TIMESERVER

Woher kommt eigentlich die Zeit?

Was sind Zeitserver?

Zeitserver (auch Timeserver) dienen zum **Synchronisieren der Uhrzeit** auf Servern, Arbeitsplatzrechnern und anderen Klienten in Netzwerken. Die aktuelle Uhrzeit wird dabei mit Hilfe einer Referenzuhr, einer Funk- oder Atomuhr, sowie des weltweiten Timeserver-Netzwerks via NTP (*Network Time Protocol*) zur Verfügung gestellt.

Der ZID der Universität Wien hat zwei neue Zeitserver in Betrieb genommen: einen GPS-Receiver, der im Neuen Institutsgebäude aufgestellt und als `ts1.univie.ac.at` erreichbar ist, sowie einen DCF77-Empfänger mit dem Hostnamen `ts2.univie.ac.at`, der das Langwellen-Zeitsignal aus Mainflingen/Deutschland auswertet und aufgrund des besseren Empfangs bei der Wiener Firma InterXion betrieben wird.

Beide Server sind Stratum 1-Uhren und frei zugänglich. Unter den Namen `ts1.aco.net` und `ts2.aco.net` sind beide Server zudem Teil des NTP-Pool (`www.pool.ntp.org`). Die bisherige Uhr unter dem Hostnamen `ts0.univie.ac.at` wurde abgebaut und verweist nun nur mehr auf einen Stratum 2-Timeserver. Es empfiehlt sich daher, `ts0.univie.ac.at` nicht mehr als Zeitserver zu konfigurieren, da dieser Host außer Betrieb gehen wird.

Der Zeitserver `ts2.univie.ac.at` verfügt über IPv6-Connectivity. Leider besteht derzeit nicht die Möglichkeit, eine IPv6-Verbindung anzubieten. Ebenso werden im NTP-Pool keine IPv6-Adressen aufgenommen.

Wie wird die Zeit „verteilt“?

Atomuhren sind derzeit die genauesten Uhren. Aus den Messwerten von über 260 Atomuhren an über 60 Instituten weltweit wird die Internationale Atomzeit als Referenzzeit festgelegt. In Österreich betreibt das Bundesamt für Eich- und Vermessungswesen mehrere Atomuhren. Ein Stratum 1-Timeserver ist direkt mit einer solchen Referenzuhr verbunden und gehört damit der obersten Schicht der Zeitserver-Hierachie an. Diese Zeit können dann Computer über das Network Time Protocol von den Stratum-1-Servern empfangen.

DCF77
Der Zeitsignalsender DCF77 ist ein Langwellensender in Mainflingen/Deutschland, der auf 77,5 kHz die Zeit der dort befindlichen Atomuhren sendet und die meisten funkgesteuerten Uhren im westlichen Europa mit der genauen Uhrzeit versorgt (`www.dcf77.de`). D steht für Deutschland, C für Langwellensender, F aufgrund der Nähe zu Frankfurt/Main sowie der Zahl 77 für die Trägerfrequenz. Die Reichweite der Bodenwelle beträgt 500 m, die der Reflexionswelle bei sehr guten Empfangsanlagen bis zu 2000 km. Wien ist weniger als 600 km von Mainflingen entfernt und es gibt normalerweise einen guten Empfang. Normale Funkuhren aus dem Supermarkt verwenden ebenfalls DCF77.

GPS-Receiver
Global Positioning System (GPS) ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung.

NTP-Pool
Das Projekt NTP-Pool ist ein Verbund von Zeitservern, die kostenlos die aktuelle Zeit über NTP (*Network Time Protocol*) im Internet zur Verfügung stellen.

Stratum 1 / Stratum 2
Stratum 1 bzw. Stratum 2 bezeichnet die Schichten der Zeitserver-Hierachie, wobei Stratum 1 höher geordnet ist als Stratum 2.

Eine kurze Geschichte über die Zeit

Wie in der Menschheitsgeschichte war auch am Computer die **Zeitmessung**[1)] ursprünglich ein lokales Ereignis. In der „echten“ Welt orientierte sich die Zeit am Sonnenstand. 12 Uhr war es, wenn die Sonne am höchsten stand, was relativ einfach mit einer Sonnenuhr festgestellt werden konnte. Die Zeit zwischen zwei aufeinander folgenden Mittags-Ereignissen wurde in 24 gleich lange Stunden eingeteilt. Um auch in der Nacht Zeit verwalten zu können, konnte man mit Hilfe des gleichen Prinzips auch eine Sternenuhr benutzen. Waren jedoch weder Sonne noch Sterne sichtbar, musste man auf periodische Abläufe zurückgreifen, deren Genauigkeit nicht gerade berauschend war und so die Messung regelmäßig in kurzen Abständen nachjustiert werden musste.

1) `www.beaglesoft.com/maintimehistory.htm`

Navigation in der Seefahrt

Diese Zeitmessung reichte auch lange Zeit für den Durchschnittsbürger aus, denn es wurde zuverlässig die Arbeitszeit und die Freizeit eingeteilt, sodass niemand übervorteilt wurde. Treibend für die Herstellung von immer genaueren Uhren war vor allem das Problem der notwendig gewordenen exakten Navigation in der Schifffahrt. Mithilfe des Sextanten, der den Sonnenstand anzeigte, einem dicken Tabellenbuch und der genauen Zeit war es möglich, die aktuelle Position zu bestimmen. Das Problem bei der Sache war die genaue Zeit und zwar bezogen auf den Ausgangspunkt der Reise, da bei monatelangen Seereisen die gemessene Zeit schon bei einer geringen Ungenauigkeit im Gang der Uhr beträchtlich von der tatsächlichen Zeit abwich. Erschwerend hinzu kam, dass das Bewegen von Uhren noch weitere Ungenauigkeit erzeugte und daher zusätzliche Herausforderungen an deren Konstruktion darstellte. Dabei ist aber noch nicht die Realbewegung der GPS-Satelliten zueinander gemeint, sondern schon alleine die Schwankung des Schiffes durch den Seegang oder die Änderung der Fahrtrichtung.

Reisen mit der Eisenbahn

Der andere angesprochene Punkt ist die **gemeinsame Zeitbasis**. Dass es bereits im Nachbarort zu einem anderen Zeitpunkt Mittag ist, war lange nicht von Bedeutung, da die Reise dorthin deutlich länger war als dieser Zeitunterschied. Das änderte sich erst mit der Einführung eines Hochgeschwindigkeitstransportsystems[2] – der Eisenbahn. Zumindest auf längeren Distanzen deutlich schneller als das bis dahin schnellste Transportmittel, das Pferd[3], hatte es einen Nachteil: Entgegenkommende Züge konnten einander nicht beliebig ausweichen. Es mussten also Fahrpläne erstellt werden. Und damit Fahrpläne funktionieren, muss an jedem Ort der Strecke die selbe Zeitbasis gelten, auch wenn damit 12:00 Uhr nicht mehr den Sonnenhöchststand bedeutet.

Durch weitere Vernetzung und Abgleich der Zeitbasen verschiedener Strecken führte diese Normierung schließlich 1884 zu einer weltweit als gültig anerkannten Zeitbasis basierend auf dem mittleren Sonnenjahr der GMT (*Greenwich Mean Time*), einer idealisierten schwankungsbereinigten Sonnenzeitmessung, die selbst zur Lokalzeit in Greenwich um bis zu 16 Minuten abweicht[4].

Damit war nun auch das Umsteigen zwischen verschiedenen Strecken nicht mehr mit Umrechnungen von einer Bahnzeit in eine andere verbunden. Die **Synchronisierung der Uhren** wurde mittels Telegrafie erledigt. Und damit die lokale Zeit nicht zu sehr von der Sonnenzeit abweicht, wurden Zeitzonen eingeführt, die lokal verordnet einen jeweils fixen Offset zur GMT darstellen[5]. „Nicht zu sehr“ bedeutet aber mancherorts trotzdem einen Versatz von mehr als drei Stunden. 1968 wurde die GMT durch die UTC (*Universal Time Coordinated*) als Zeitbasis abgelöst. Diese wird nun nicht mehr durch die reine Beobachtung der Sonnenzeit bestimmt, sondern basiert auf einem weltweiten Verbund von Atomuhren.

Damit diese Zeitbasis nicht von der durch die Verlangsamung der Erdrotation verursachten, entschleunigten Sonnenzeit in Greenwich wegdriftet, sind Schaltsekunden vorgesehen, wenn GMT mehr als 0,9 Sekunden von der UTC[6] abweicht. In einem solchen Fall hat die letzte Minute des Jahres dann 61 Sekunden. Durchschnittlich wird alle 2 Jahre solch eine Sekunde geschaltet und bisher gab es seit 1972, dem Jahr mit der ersten Schaltsekunde, insgesamt 24 zusätzliche Sekunden. Zuletzt war dies am 31.12.2008 23:59 UTC, das entspricht dem 1.01.2009 00:59 MEZ, der Fall.

Computer und Zeit

Eine ähnliche, wenn auch deutlich rasantere, Entwicklung machte die Zeitmessung am Computer durch. Beim frühen Personal Computer wurde die Uhr am Arbeitsrechner bestenfalls minutengenau eingestellt und je nach verbauter Hardware änderte sich die Zeitdifferenz zur Pendeluhr an der Wand mehr oder weniger. Das war aber kein Problem, solange es nur darum ging, die Reihenfolge der Ereignisse am Rechner zu dokumentieren, eventuell verknüpft mit der ungefähren Zeitangabe, wann ein Eintrag erfolgte. Die Kollegin am Nachbarrechner hatte ebenfalls ihre eigene Zeit, aber beide Rechner zeigten in der Regel den selben Tag an, was für den Versand von Briefen und Rechnungen vollkommen zufriedenstellend war.

Wie auch heute wurde die Systemzeit am PC meist in einer RTC (*Real Time Clock*)[7] gehalten. Beim Hochfahren des Rechners übernimmt das Betriebssystem die aktuelle Zeit der RTC und verwendet meist die CPU, um während des Betriebes die Zeit zu bestimmen. Beim Herunterfahren des Rechners wird dann die Zeit vom Betriebssystem in der RTC gesetzt. Die meisten RTCs halten die Zeit als Unix-Zeit[8] vor, das ist die Anzahl der Sekunden seit dem 1. Januar 1970 00:00 Uhr UTC, wobei Schaltsekunden nicht mitgezählt werden. Dieses Startdatum wird auch als Epoche bezeichnet. Insgesamt steht ein 32 bit-Register für das Zählen der Sekunden zur Verfügung. Soll damit eine ganze Zahl mit Vorzeichen dargestellt werden, so können insgesamt 2^{31-1} das sind 2.147.483.647 Sekunden gezählt werden, bevor die Zahl ins Negative kippt. Das passiert am 19. Januar 2038 um 03:14:07 Uhr, eine Sekunde später wäre dann am Rechner der 13. Dezember 1901 20:45:52. Dieses Problem, auch *Jahr-2038-Problem* bezeichnet, wird natürlich schon einige

2) http://de.wikipedia.org/wiki/Liste_der_Geschwindigkeitsweltrekorde_für_Schienenfahrzeuge

3) http://equivetinfo.de/html/eckdaten_pferd.html

4) http://de.wikipedia.org/wiki/Greenwich_Mean_Time

5) http://de.wikipedia.org/wiki/Zeitzonen

6) http://de.wikipedia.org/wiki/UTC

7) http://de.wikipedia.org/wiki/Echtzeituhr

8) http://de.wikipedia.org/wiki/Unixzeit

9) www.rfc-editor.org/rfc/rfc1305.txt

10) http://support.microsoft.com/?kbid=262680

11) http://wiki.ubuntuusers.de/Systemzeit

12) www.metrologie.at/index.html/homepage_messeichwesen_016.htm

13) www.pool.ntp.org

Jahre davor relevant, da auch immer wieder Tage in der Zukunft berechnet werden müssen. Aber noch lässt uns dieses Problem kalt wie seine Entsprechung, die Y2K, im Jahr 1998.

Zeit in Netzwerken

Mit dem ersten Aufkommen von lokalen Netzwerken war es schließlich möglich und manchmal auch notwendig, dass die Uhren der vernetzen Rechner dieselbe Zeit anzeigten. Technisch wurde das Problem gelöst, indem die aktuelle Zeit von einem Nachbarrechner automatisch übernommen wurde. Damit entfiel die lästige Datums-Einstellung am Arbeitsplatz-PC und es war nur mehr die Uhr des zentralen Zeitservers zu warten. Schließlich wurden, wie nach der Gründerzeit die Eisenbahnstrecken auch, die lokalen Computernetzwerke zu größeren Verbünden zusammen geschaltet.

Große Netzbetreiber boten für viel Geld diese Dienstleistungen an und viele von diesen verschwanden auch wieder, der Rest ging praktisch im in der Zwischenzeit ins Leben gerufenen Netz der Computernetze, dem Internet auf. Auch die korrekte Zeiteinstellung am Rechner hat sehr an Bedeutung gewonnen. Nicht nur rein administrative Daten, wie die Zeitstempel in Logfiles, sind nur dann einfach verwertbar, wenn die interne Uhr stimmt, auch Applikationen wie Erinnerungsfunktionen im Kalender verlassen sich auf eine richtige Uhrzeit. Dies geht so weit, dass Sicherheitsprotokolle den Verbindungsaufbau zu einem anderen Rechner ablehnen, wenn die Zeiten auf beiden Hosts eine zu große Differenz aufweisen.

Timeserver

Damit die Zeit automatisch eingestellt werden kann, ist es notwendig, ein entsprechendes Verfahren zu spezifizieren. Im Internet ist die Synchronisierung der Zeit in einem eigenen Standard[9]geregelt. Dazu werden im Internet Server betrieben, welche als Dienst die Zeitsynchronisierung anbieten. Naheliegenderweise heißen diese Server Timeserver. Timeserver bilden eine Hierarchie, die durch das so genannte *Stratum* (übersetzt Schicht) bezeichnet wird. Stratum 0, also die oberste Schicht, bilden die Atomuhren. Die Server in Stratum 1 holen ihre Zeit von einer Stratum 0-Uhr. Der Transport ist dabei unerheblich, es können die Uhren direkt angeschlossen sein oder die Zeit auch via Mittelwellenfunk oder GPS-Signal übermittelt werden. Und letztendlich holen Stratum 2-Server ihre Zeit von einem Stratum 1-Server. Dabei werden alle Server so konfiguriert, dass die Übertragungslatenzen entfernt werden. So kann jeder Host im Internet durch das Angebot der Dienste von Timeservern seine Zeit akkurat halten. Und weil diese Synchronisierung so wichtig ist, hat jeder Anbieter eines neueren Betriebssystem auch automatisch einen Server für den Zeitabgleich konfiguriert, auf den der Client voreingestellt ist.

Ein Nachteil dieser Grundeinstellung ist, dass der Zeitserver meist sehr weit entfernt ist und daher die Latenz der Antworten hoch und relativ weit gestreut ist. Daher ist es sinnvoll, einen oder mehrere Server in der Nähe zu konfigurieren. Diese Nähe sollte auch das erste Auswahlkriterium sein. Ein gut gewarteter Stratum 2-Timeserver im eigenen Netz liefert bessere Ergebnisse, als in Stratum 1-Server am anderen Ende der Welt.

Zur Auswahl steht ein großes Angebot: Die Universität Wien bietet ihren Usern die beiden Server `ts1.univie.ac.at` und `ts2.univie.ac.at` sowie die beiden frei zugänglichen Server `ts1.aco.net` und `ts2.aco.net` an. Microsoft verweist auf fremde Listen von Zeitservern[10] und die Ubuntu-Community bietet ihren Usern eigene Informationen[11] an. Das Bundesamt für Eich- und Vermessungswesen stellt seine an die eigenen Atomuhren angeschlossenen Zeitserver zur Verfügung[12]. Wenn Sie eine selbstorganisierende Quelle für öffentliche Zeitserver aus Österreich konfigurieren möchten, so konfigurieren Sie einfach `0.at.pool.ntp.org`, `1.at.pool.ntp.org`, `2.at.pool.ntp.org` und `3.at.pool.ntp.org` als Timeserver [13].

Bitte beachten Sie, dass Sie hier eine Gratisdienstleistung in Anspruch nehmen, die nicht über Gebühr strapaziert werden sollte. Daher gehört es zum guten Ton, bestimmte Konfigurationsrichtlinien einzuhalten. Die Standardkonfigurationen der Timeserver-Klienten entspricht bereits diesen Anforderungen: Die Verwendung von `iburst` soll `burst` vorgezogen werden, als Werte für die Parameter `minpoll` und `maxpoll` sollen 64 Sekunden bzw. 1024 Sekunden konfiguriert werden, ein ntp-Klient soll die KOD-Nachrichten des Servers beachten und die Timeserveradressen sollen immer als Hostnamen und nie als IP-Adressen konfiguriert werden.

Andreas Papst

Eintragen eines Timeservers unter Windows 7

Klicken Sie auf die Uhrzeit rechts in der Taskleiste und dann auf *Datum/Uhrzeit ändern*. Wählen Sie die Registerkarte *Internetzeit* und klicken dort auf *Einstellungen ändern*. Geben Sie in das Feld *Server* einen Timeserver, z. B. `ts1.univie.ac.at` ein.