

Zeitschrift: Zeitlupe : für Menschen mit Lebenserfahrung
Herausgeber: Pro Senectute Schweiz
Band: 82 (2004)
Heft: 3

Artikel: Von Viren und Würmern
Autor: Honegger, Annegret
DOI: <https://doi.org/10.5169/seals-722627>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 04.04.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

Von Viren und Würmern

Das Internet wird zunehmend unentbehrlich. Gleichzeitig sorgen Viren und andere Schädlinge immer wieder für negative Schlagzeilen. Doch es gibt Möglichkeiten, den Computer sicherer zu machen.

VON ANNEGRET HONEGGER

Kaum jemand, der heute nicht die grossen Vorteile des Internets nutzt. Wo sonst gibt es Millionen von Informationen zu allen erdenklichen Themen? Wie sonst kann man in Sekundenschnelle mit Bekannten und Unbekannten rund um den Erdball kommunizieren? Surfen und E-Mailen sind aus der Gesellschaft nicht mehr wegzudenken.

Über 172 Millionen Computer sind heute am Internet angeschlossen. Diese grosse Verbreitung birgt Chancen – und Gefahren. Denn nicht nur das «Gute», sondern auch das «Böse» breitet sich über das neue Medium rasend schnell aus. Schlagzeilen machen etwa bösartige Computerviren, die unzählige Rechner zum Absturz bringen, oder Betrüger, die Benutzerinnen und Benutzern via Internet das Geld aus der Tasche ziehen.

Wer sich im Internet bewegt, öffnet seinen Computer bewusst für gewünschte Daten und Dokumente, wie etwa Webseiten und E-Mails. Die gleichen Kanäle ermöglichen aber auch ungewollten Besuch auf dem eigenen Rechner – falls dieser nicht ausreichend geschützt ist. Ist die Datenautobahn also gefährlich, weil an jeder Ecke Wegelagerer mit unlauteren Absichten lauern?

Michael Näf von der Forschungsgruppe für Informationssicherheit an der ETH Zürich winkt ab: «Wie im sonstigen Leben müssen wir zuerst lernen, mit den Gefahren in diesem neuen Medium angemessen umzugehen. Vielen Leuten fehlt dazu einfach noch die Erfahrung.» Im Alltag etwa wissen wir genau, welche Risiken wir eingehen, wenn wir ohne Helm Velo fahren oder die Handtasche im Gedränge nicht im Auge behalten. Auch Einbrecher haben in unserer Wohnung dank guten Schlössern oder einer Alarmanlage kein leichtes Spiel. Im Internet

aber verhalten wir uns aus Mangel an Wissen oft fahrlässig.

Das grösste Problem für private Nutzer sind fremde Daten und Programme. Diese können auf den eigenen Rechner gelangen, sobald man sich beim E-Mailen oder Surfen ins Internet einwählt. «Hacker nutzen Sicherheitslücken im Betriebssystem, im Web-Browser und anderen Anwendungen – und nicht zuletzt die Naivität vieler Benutzerinnen und Benutzer», sagt Michael Näf. Einigen geht es nur darum, das eigene Werk möglichst weit zu verbreiten. Andere wiederum spionieren fremde Rechner aus, bringen sie zum Absturz oder schädigen Daten.

Die Plagegeister tarnen sich

In vielen Fällen wissen die Benutzer nicht einmal, dass sie fremde Programme auf den eigenen Rechner herunterladen. Damit Webseiten sich bewegen, blinken oder tönen, wird zum Beispiel mit aktiven Elementen wie JavaScript oder ActiveX gearbeitet. Diese kleinen Programme gelangen mit dem Inhalt der Webseite auf den eigenen Computer. Nicht immer sind diese Elemente harm-

los – sie können unbeabsichtigte Fehler enthalten oder aber gezielt schädliche Funktionen. Ebenso heimtückisch sind so genannte Dialer, die meist über abgerufene Erotik-Seiten teure Telefonverbindungen vom persönlichen Rechner ins Internet herstellen. Besonders hinterhältig: Oft verbergen sich die Plagegeister hinter einer durchaus nützlichen Funktion wie etwa einem Bildschirmschoner. So getarnte Übeltäter heissen nach der griechischen Sage «Trojanische Pferde».

Die bekanntesten Schädlinge sind Viren und Würmer. Auch sie sind kleine Programme, die meist als E-Mail-Anhänge auf den Computer geraten. Ähnlich wie biologische Viren im Körper nisten sie sich im System ein und verbreiten sich dort selbstständig. Ihre Wirkung reicht von witzig über nervenaufreibend bis katastrophal. Harmlosere Viren verlangsamen den Computer, kehren die Maussteuerung um oder stellen die Bildschirmanzeige auf den Kopf. Schlimmere verschieben oder löschen Dateien, verschicken selbstständig E-Mails an Adressen im persönlichen Adressbuch oder löschen die ganze Festplatte. Viren können sich fast überall verbergen, sogar in E-Mails im HTML-Format oder als Makro-Viren in Word-Dokumenten. Ein falscher Klick genügt, und die Plagegeister starten ihre fiesen Funktionen.

Genau bei diesem Klick setzen die Tipps an, die Experte Näf empfiehlt. «Die wichtigste Massnahme gegen die Gefahren aus dem Internet kostet nichts: Eine Portion Misstrauen und gesunder Menschenverstand.» Bei E-Mails mit eigenartigen Inhalten oder unbekanntem Absendern ist immer Vorsicht geboten. Wieso schickt mir der Jass-Kollege eine E-Mail mit dem Betreff «I LOVE YOU»? Warum sollte ich mir die Urlaubsfotos von wildfremden Menschen anschauen wollen? Da sich Viren selbst verschicken

SICHERHEITS-LINKS

Sicherheit im Internet (mit Glossar):

www.internet-kompetenz.ch
www.bsi-fuer-buerger.de
www.microsoft.ch/de/security

Viren-Liste:

www.pctip.ch/helpdesk/virenticker

Hoax-Liste:

www.tu-berlin.de/www/software/hoax.shtml

Antiviren-Software:

kostenpflichtig: www.mcafee.com,
www.symantec.com, www.avp.ch;
gratis: www.free-av.de

Personal Firewall:

www.zonelabs.com

BILD: PRISMA

können, ist auch ein bekannter Absender keine Garantie für einen sauberen Inhalt. Es gilt: ungelesen löschen.

Ebenfalls in den virtuellen Papierkorb gehören Kettenbriefe, die um Geld bitten. Etwa «Helfen Sie unserer krebskranken Tochter» oder «Legen Sie Ihr Geld todsicher in Nigeria an». Auch die so genannten Hoaxes, gefälschte Warnungen vor Viren und sonstigen Schrecknissen, sind an sich nicht schädlich, aber lästig. So plausibel sie klingen, so unecht sind sie meistens. Tausendfach weitergeleitet – und sei es in bester Absicht –, belasten sie nur Postfächer und Nerven. Ein Blick auf eine Hoax-Liste im Internet zeigt schnell, ob sich eine Meldung bereits als falsch erwiesen hat.

Sicherheit kann auch etwas kosten

Eine weitere Massnahme, die mit Technik wenig zu tun hat, ist der gesunde Verzicht. Viele Multimedia-Spielereien sind zwar lustig, aber nicht wirklich nötig. Der Web-Browser bietet entsprechende Sicherheitseinstellungen, die steuern, dass zum Beispiel JavaScript und ähnliche Programme nicht heruntergeladen und ausgeführt werden dürfen.

«Antiviren-Software ist heute ein Muss für jeden Computer», betont Michael Näf. Diese Programme prüfen automatisch alle vom Internet heruntergeladenen Dateien oder frisch gestarteten Anwendungen. Sie sind einfach in der Bedienung und können gegen Gebühr oder gratis vom Internet geladen werden. Wichtig ist, die Software mit den Updates zu aktualisieren. «Schliesslich», so Michael Näf, «warten wir auch unser Auto regelmässig und sind uns im Klaren, dass Sicherheit etwas kostet.» Achtung: Kein Software-Hersteller verschickt seine neusten «Sicherheits-Pflaster» (Patches) per E-Mail – so tarnen sich Viren.



■ SCHMERZENDE FUßSOHLEN, HORNHAUT...

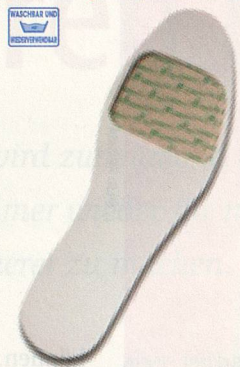
Unsere Podologen beantworten Ihre Fragen



Was ist das Fußsohlenpolster?
Der Fuß besitzt einen natürlichen Stoßdämpfer, das sogenannte **Fußsohlenpolster**. Es kann Schocks ertragen, die 8 Mal dem Gewicht des Körpers entsprechen. Das **Fußsohlenpolster** gewährt die "Verteilung des Gewichtes" unter dem Vorderfuß. Diese leistungsstarke, schützende Rolle ergibt sich durch die Struktur aus flüssigen und fetten Massen, zurückgehalten in Kollagen-Fasern.

Was ist das Epithelium 26*?
Leider stellt man sehr häufig fest, dass im Alter eine unwiderrufliche Veränderung des Fußsohlenpolsters entsteht, die äußerst starke Schmerzen unter dem Vorderfuß verursacht und sich Hornhaut bildet. Epitact und ihre zwei Partner-Podologen haben von diesem Zustand Kenntnis genommen und nach langjähriger Forschung ein neues, bahnbrechendes Material entwickelt: **Das Epithelium 26*, Gel aus patentiertem Silikon, ein vollwertiger Ersatz für das Fußsohlenpolster, natürlich und gesund.** Die Integrierung des Epithelium 26* in die Sohlen ergibt ein ausserordentliches Resultat!

Was ist das AeroShoes?
Dieses Material wurde speziell für die Aufnahme und Abgabe von Feuchtigkeit hergestellt. ideal, um das Feuchtigkeitsgefühl durch Schweißabsonderung in den Schuhen zu vermeiden. Die Sohle kann ihr eigenes Gewicht in Wasser aufnehmen.



- Die Sohlen mit Epithelium 26***
Die Sohlen sind aus 2 leistungsstarken Materialien hergestellt: das Epithelium 26* und das AeroShoes*.
- Sie sind diskret und dünn und sie können in den üblichen Schuhen getragen werden.
 - In den **Schuhgrößen 34 bis 45 erhältlich.**
 - Sie haben **eine lange Benutzungsdauer**
 - Sie sind **bei 30° in der Maschine waschbar.**

Ihr Podologe berät Sie gerne

FRANZÖSISCHE HERSTELLUNG CE Mehr als 3000 Partner-Podologen



SUNAPTIS Alleinvertretung für die Schweiz

Mit frankiertem Kouvert senden an:
SUNAPTIS SA • CP 6268 • 1211 GENÈVE
Tel. 022 363 07 13 • Fax 022 363 07 14 • E-mail : alicegohl@sunaptis.com

<input type="checkbox"/>	1 Paar Sohlen mit Epithelium 26* Ref. 0621	54,00 CHF
	Versandkosten	5,00 CHF
	Total Betrag	59,00 CHF
<input type="checkbox"/>	1 Paar tragen während das andere gewaschen wird 2 Paar Sohlen mit Epithelium 26*	108,00 CHF
	Versandkosten	GRATIS
	Total Betrag	108,00 CHF
<input type="checkbox"/>	Umkreisen Sie die gewünschte(n) Größe(n) 34 35 36 37 38 39 40 41 42 43 44 45	
<input type="checkbox"/>	Gratiskatalog	

NAME..... Vorname.....
 Adresse.....
 PLZ. Ort.....
 Tel. Geburtsdatum

Noch mehr Sicherheit bietet eine Personal Firewall. Dies ist eine für Heimwender vereinfachte Version der «Brandmauern», mit denen Unternehmen ihre Netzwerke schützen. Ganz im Sinne der mittelalterlichen Burgmauer überwacht diese Software den Datenverkehr vom und ins Internet. Die Firewall warnt, wenn Pakete ohne ersichtlichen Grund in den Computer hinein- oder von diesem ins Internet hinauswollen. Was einfach klingt, geht aber nicht ohne technisches Wissen und Interesse bezüglich der Einstellungen und der richtigen Reaktion auf allfällige Meldungen. Michael Näf betont: «Ein gut konfiguriertes System mit einer aktuellen Antiviren-Software braucht nicht unbedingt eine Firewall.»

Eine Patentlösung für Sicherheit im Internet gibt es also nicht. Massgebend sind die persönlichen Anforderungen und die eigene Risikobereitschaft. Vorsicht und gesunder Menschenverstand sind ebenso wichtig wie das technische Wissen. Regelmässige Sicherheitskopien (Backups) der Daten können im Notfall den Schaden begrenzen. «Weil immer mehr Menschen auf sichere Computer angewiesen sind, muss Sicherheit über kurz oder lang auch für Hersteller und Anbieter einen grösseren Stellenwert bekommen», hofft Michael Näf. Der Experte stellt sich vor, dass es bald öffentliche Sensibilisierungs-Kampagnen à la Suva oder Stop Aids geben wird. Zum Beispiel: Ohne Schutz kein Klick.

LITERATUR:



Michael Näf, Patrick Streule, Werner Hartmann: Risiko Internet? Sicherheitsaspekte bei der Internet-Benutzung. Orell Füssli Verlag, 2000. 158 S., CHF 43.-

Das Buch vermittelt klar und verständlich langlebige Konzepte und Fachwissen, um die Risiken im Internet zu beurteilen und einzuordnen.



Heini Lüthy: Das Internet sinnvoll nutzen. K-Tipp Ratgeber 15, 2003. 143 S., CHF 30.-

Mit praktischen Tipps zu Musik, Bildern und Videos bis zu E-Commerce und Sicherheit. Bestellatalon Seite 68.