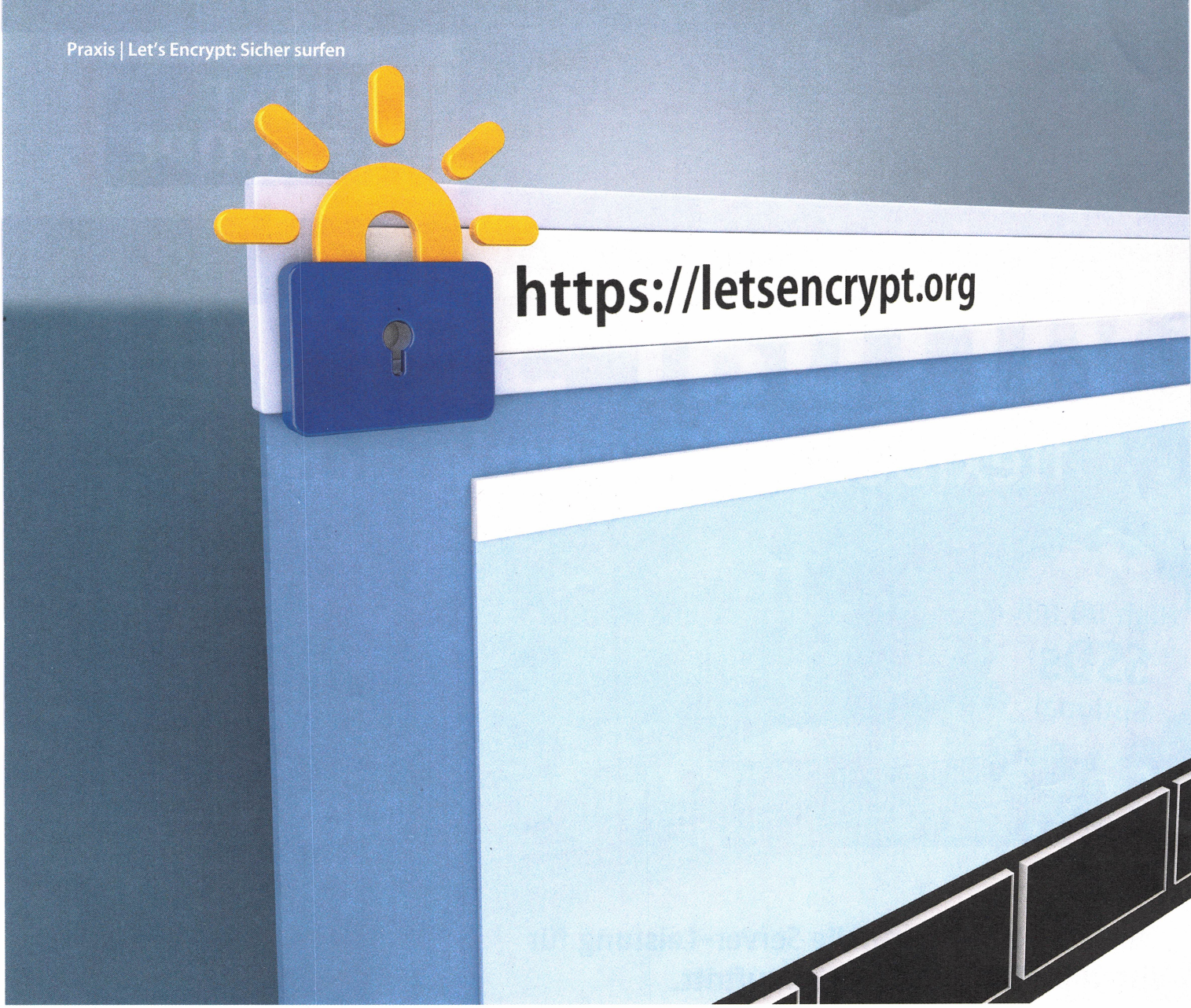


Johannes Merkert, Jan Schüßler

Aber sicher!

Verschlüsselt surfen mit HTTPS Everywhere und PassSec+

Ihr Webbrowser spricht mit den Seiten, die Sie ansurfen, verschlüsselt – aber leider nur im Idealfall. Ein paar einfache Mittel schützen nicht nur Ihre Privatsphäre, sondern warnen auch vor Angriffen auf Ihr Bankkonto und Ihre Online-Einkäufe.

Eigentlich sollte es für Betreiber von Webseiten zum guten Ton gehören, alle Inhalte über eine verschlüsselte Verbindung zum Besucher zu übertragen. Manchmal sprechen durchaus triftige Gründe dagegen – zum Beispiel Werbeanbieter, die keine Verschlüsselung unterstützen. In einigen Fällen werden ganze Internet-Sites wahlweise unverschlüsselt oder verschlüsselt angeboten. Letzteres erkennt man daran, dass vor der eigentlichen Adresse das Präfix https:// steht.

Überall, bitte!

Um Websites grundsätzlich gesichert abzurufen, müssten Sie vor deren Adressen von Hand „https://" eintippen, denn: Nicht jeder Betreiber, der auch eine verschlüsselte Übertragung anbietet, leitet Ihren Browser automatisch zum gesicherten Angebot.

Das Plug-in HTTPS Everywhere gibt es auf dem PC für die Browser Chrome, Firefox und Opera. Entwickelt wurde es von der Electronic Frontier Foundation (EFF), die auch die Let's-Encrypt-Kampagne mitinitiiert hat. Es nimmt Ihnen die Handarbeit ab: Sie tippen URLs wie gewohnt ohne https:// in die Adresszeile ein; falls sich die Seite auch verschlüsselt abrufen lässt, leitet das Plug-in automatisch auf die sichere Verbindung um. Klicken Sie innerhalb der Seiten auf Links, landen Sie immer bei der https-Seite – egal, ob der ur-

HOST EUROPE

Virtual Server

flexibel und günstig sichern

High I/O mit **SSDs** optional

Nutzen sie jetzt virtuelle Server-Leistung für Ihren professionellen Webauftritt.

- ✓ Ohne Einrichtungsgebühr und Mindestvertragslaufzeit
- ✓ Aktuellste OS wie Debian 8 oder Windows Server 2012 R2
- ✓ Individuelle Konfiguration durch Root-Zugriff
- ✓ Gratis Add-ons wie SSL, Plesk 12, Backup uvm.

schon ab **€ 12,99** mtl.

Starter	Advanced	Expert	Unlimited
CPU: 1 vCore	CPU: 2 vCores	CPU: 4 vCores	CPU: 8 vCores
RAM: 2 GB	RAM: 4 GB	RAM: 8 GB	RAM: 16 GB
Disk: 150 GB SATA	Disk: 300 GB SATA	Disk: 750 GB SATA	Disk: 1000 GB SATA
€12,99 /mtl.	Snapshot: 1 inklusive	Snapshots: 2 inklusive	Snapshots: 5 inklusive
	€16,99 /mtl.	SSL-Zertifikat: Domain SSL inklusive	SSL-Zertifikat: Domain SSL inklusive
		€29,99 /mtl.	**€49,99** /mtl.

Jetzt informieren unter: **www.hosteurope.de/vserver** **02203 1045-7810**

24/7 In-house Support • 99,95% Uptime-SLAs • Exzellenter Service

sprüngliche Link dorthin geführt hätte oder nicht.

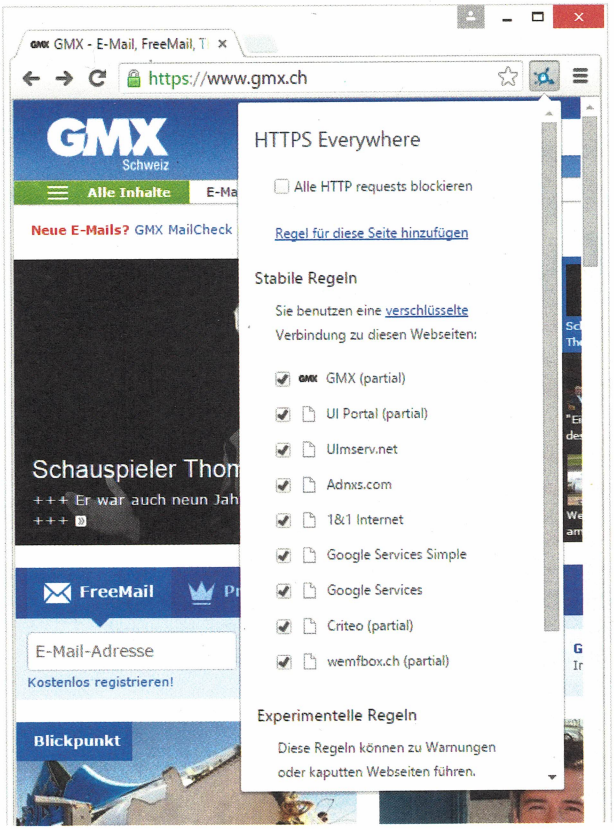
HTTPS Everywhere greift auf eine umfangreiche Liste von Websites zurück, die verschlüsselt erreichbar sind. Sie wird von der EFF laufend gepflegt. Anwender müssen sich weder um die Aktualisierung der Liste noch um die Funktion des Plug-ins kümmern – alles geschieht automatisch im Hintergrund.

Das Plug-in steht für alle drei Browser im jeweiligen Erweiterungs-Store unter dem Menüpunkt „Erweiterungen" zur Installation bereit. Einfacher ist es, den direkten Installations-Link auf der Homepage der EFF zu klicken (siehe c't-Link). Die Seite erkennt automatisch, welchen Browser Sie verwenden, und führt mit wenigen Klicks durch die Installation des Plug-ins.

PassSec+

HTTPS Everywhere leitet stets auf verschlüsselte Verbindungen, wenn die Seitenbetreiber eine anbieten. Das ändert allerdings nichts daran, dass es noch viele unverschlüsselte Webseiten gibt – mitunter sogar welche, auf denen Sie zum Login Benutzername und Passwort eingeben sollen. Geben Sie auf einer solchen Webseite Ihre Login-Daten ein, werden auch diese unverschlüsselt übertragen und Angreifer können diese mitlesen.

GMX gehört zu den vielen Websites, für die HTTPS Everywhere eine Regel mitbringt. Durch das Plug-in rufen Sie automatisch die verschlüsselte Version auf, ohne die Adressleiste im Blick behalten zu müssen.

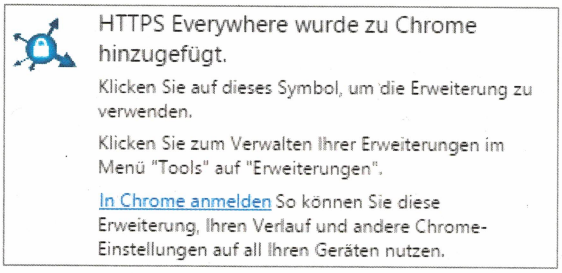


HTTPS Everywhere installieren

in Chrome

Schritt 1: Die Homepage der Erweiterung HTTPS Everywhere (siehe c't-Link) erkennt Ihren Browser und lässt Sie das passende Plug-in per Klick installieren.

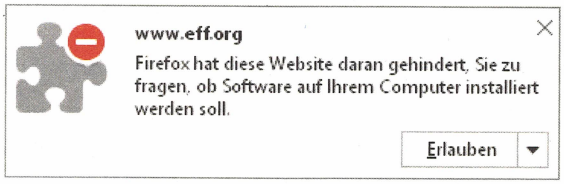
Schritt 2: Nach dem Klick auf den Installations-Link bittet Chrome um Erlaubnis, HTTPS Everywhere zu installieren.



Schritt 3: Wenige Sekunden später ist HTTPS Everywhere in Chrome installiert und einsatzbereit.

in Firefox

Schritt 1: Rufen Sie die Homepage von HTTPS Everywhere auf (siehe c't-Link) und klicken Sie auf „Install in Firefox".



Schritt 2: Daraufhin bittet Firefox Sie, die Installation durch einen Klick auf „Erlauben" zuzulassen.

Schritt 3: Kurze Zeit später starten Sie die eigentliche Installation.

Schritt 4: Bei Firefox wird HTTPS Everywhere erst nach einem Neustart des Browsers aktiv.

Das Plug-in PassSec+ hilft Ihnen dabei, an dieser Stelle keine Fehler zu machen. Zur Zeit ist es nur für Firefox zu haben. PassSec+ prüft, wie das Passwort einer Login-Seite übertragen wird, und färbt das Eingabefeld passend ein. Falls sich die Seite mit einem EV-Zertifikat ausweisen kann – also mit einem Zertifikat, das der Inhaber nur nach detaillierter Prüfung seiner Identität bekommt – , umgibt das Feld ein grüner Rahmen, begleitet von einem grünen Schloss. So sollte es bei einer Bank oder bei PayPal immer aussehen.

Hat die Zertifizierungsstelle die Identität des Anbieters einer verschlüsselten Seite nur automatisch geprüft, rahmt PassSec+ das Passwortfeld gelb ein. Bevor Sie dort Ihr Kennwort eingeben, fordert Sie das Plug-in dazu auf, die URL zu prüfen: Passt die angezeigte Adresse im Browser zu der Seite, auf der Sie sich gerade wähnen? Sobald Sie das bestätigen, färbt sich der Rahmen grün.

Passwortfelder auf unverschlüsselten Seiten hebt PassSec+ deutlich in Rot hervor. Das Plug-in wird Sie letztlich nicht daran hindern, in gelb oder rot markierte Felder Ihre Login-Daten einzugeben – die deutliche Warnung und die angezeigten Erklärungen halten Sie aber davon ab, Fehler zu machen.

Das Plug-in wurde von der „Forschungsgruppe SECUSO – Security, Usability and Society" an der TU Darmstadt entwickelt und steht auf deren Webseite zum Download bereit (siehe c't-Link). Beim Klick auf den Link am Ende der Seite bietet Firefox direkt an, das Plug-in zu installieren – der weitere Vorgang entspricht dem für HTTPS Everywhere.

Vertrauen ist gut …

… aber Kontrolle ist besser. Wenn Sie auf Internetseiten mit wichtigen Login-Daten wie etwa einem Mail-Passwort oder Ihrer PIN fürs Online-Banking hantieren, möchten Sie nicht nur sicherstellen, dass die Verschlüsselung funktioniert, sondern auch, dass Ihr Browser wirklich mit Ihrer Bank redet.

Gängige Browser zeigen Informationen zur Verschlüsselung und zum verwendeten Zertifikat an. In Chrome und Firefox zeigt ein Klick auf die Weltkugel beziehungsweise das Schloss links neben der Adresse an, ob mit der Identität der Website alles stimmt. Wenn nicht, hat das oft banale Ursachen wie ein abgelaufenes Zertifikat oder ein gültiges, das aber nicht zur angesurften Adresse passt. Allerdings kann es auch auf einen Angriff hindeuten.

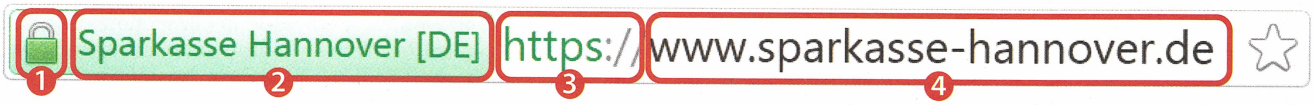
In solchen Fällen fehlt der Beweis für die Echtheit einer Seite, weshalb der Browser statt der gewünschten Website einen Warnhinweis einblendet. Darin steht, warum die Echtheit der Seite nicht überprüfbar ist und der Zugriff blockiert wird.

Meistens zeigen solche Warnmeldungen auch eine Option, die Seite trotz aller Sicherheitsbedenken zu besuchen – lassen Sie die Finger davon! Die Funktion ist ausschließlich Sonderfällen vorbehalten, die etwa in firmeninternen Netzen vorkommen. Doch selbst dort gilt: Fragen Sie den IT-Verantwortlichen Ihrer Firma, ob die Sicherheitswarnung wirklich normal ist! Gerade in Firmennetzwerken kann hinter einer solchen Warnung auch ein Angriff von Kriminellen oder Spionen stecken, die sich die Sorglosigkeit eines Mitarbeiters zunutze machen wollen.

(jss@ct.de)

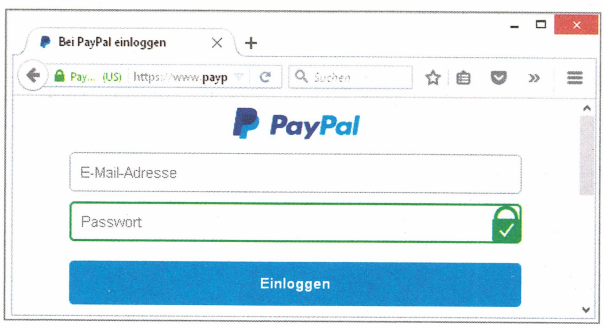
c't Alle Plug-ins: ct.de/yvxb

Adresszeile Ihres Browsers bei korrekter Verschlüsselung

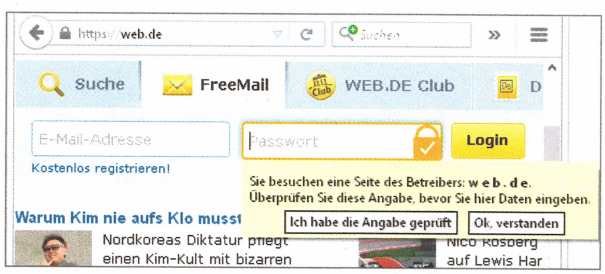


Die Adresszeile zeigt gleich vier starke Indizien für eine sichere Online-Verbindung zu Ihrer Bank: 1. grünes Schloss-Symbol, 2. passender Zertifikats-Besitzer, 3. „https"-Präfix und 4. eine passende Internet-Adresse.

So funktioniert PassSec+



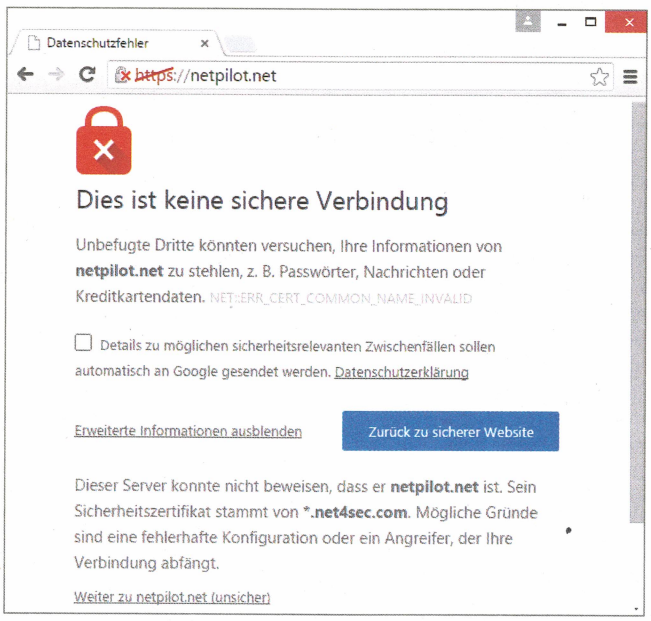
So soll es sein: Ist das Passwortfeld grün, können Sie darauf vertrauen, dass Ihre Login-Daten sicher übertragen werden.

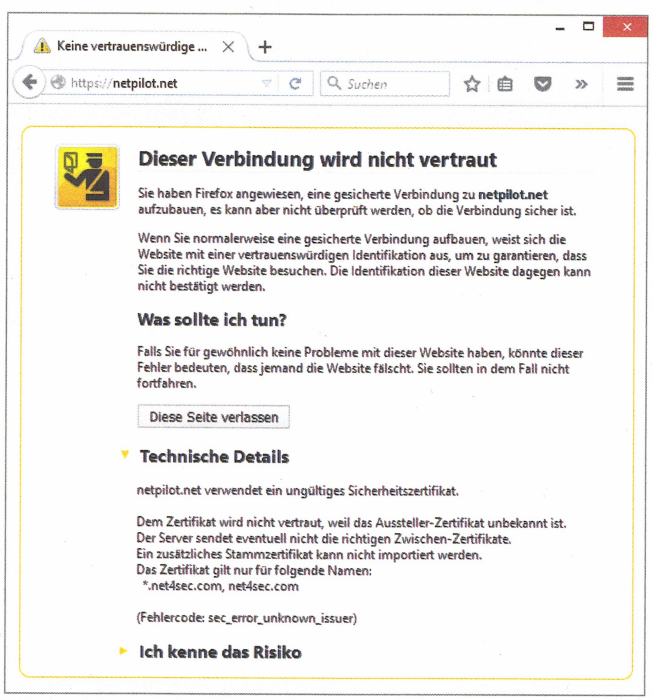


Besitzt eine Website nur ein einfaches, automatisch ausgestelltes Zertifikat, fordert PassSec+ Sie dazu auf, die Adressangaben zu vergleichen.

Hier wurde web.de über eine unverschlüsselte Verbindung aufgerufen. Angreifer könnten Ihr Passwort mitlesen – weshalb PassSec+ vor der Eingabe warnt.

Fehlermeldungen in Chrome und Firefox





Wenn das Zertifikat einer verschlüsselten Seite unstimmig ist, blockieren die Browser den Zugriff. Hier ist das Zertifikat zwar gültig – nur eben nicht für die aufgerufene Adresse.

c't