



Im Internet lauern Gefahren: Kriminelle versuchen, an die persönlichen Daten der Nutzer zu gelangen.

Fotos: Carsten Riedl

Gesundes Misstrauen hilft im Netz

Frauenkulturtage Geballte Information prasselte auf die Zuhörerinnen im Kirchheimer Spitalkeller nieder. Sicher im Netz mit PC, Smartphone und Tablet war das Thema von Jutta Bundschuh bei der vhs-Veranstaltung. *Von Iris Häfner*

Sicher werden im Netz und Hilfe zur Selbsthilfe – das waren die zentralen Anliegen von Jutta Bundschuh für den Abend im Rahmen der vhs-Donnerstagsvorträge und der Frauenkulturtage. Rund ums Thema Internet gibt die Referentin viele Kurse an den Volkshochschulen in Kirchheim und Filderstadt, aber auch an Grundschulen bei Dritt- und Viertklässlern in Esslingen.

„Ich kann ihnen leider keine konkreten Gefahrenquellen nennen, die ändern sich ständig“, nahm sie den Teilnehmerinnen gleich zu Beginn ihres mit Informationen vollgespickten Vortrags jegliche Illusion. Anhand eines Schaubilds zeigte sie den Aufbau und vor allem die Vernetzung der einzelnen Geräte auf. „Der Router ist die Verbindung nach außen. LAN nennen wir die Kabelverbindung, WLAN ist drahtlos“, erklärte sie die Technik, mit der die Nutzer arbeiten. Der Browser ist das Tor ins Internet. „Mit dem kommen wir raus. Da sind unsere Daten hinterlegt: Adresse, wie lange wir im Netz waren, die Rechnungen und dergleichen. Der Server, egal ob in Schweden oder USA steht, protokolliert, was gesucht wurde“, verdeutlichte sie. Deshalb landen die Cookies – „diese Schokoladenkekse“ – auf dem heimischen PC oder dem Smartphone. „Ohne die funktioniert es nicht“, hat sie Verständnis für diese Art von Werbung, mit der die Firmen ihr Geld verdienen. „Wenn man sie ablehnt, funktionieren die Programme manchmal gar nicht“, erklärte sie.

Der Browser, beispielsweise Mozilla oder Internet Explorer,

ist die Schnittstelle zwischen innen und außen. Hat jemand Musik illegal vom Netz heruntergeladen, kann beim Gericht der Antrag auf Server-Protokolle gestellt werden, damit die Polizei ermitteln kann. „Vorratsdatenspeicherung ist in Deutschland aber eigentlich nicht erlaubt. Im Moment geht das gar nicht“, sagte Jutta Bundschuh.

Wer seine Spur im Internet nicht so deutlich preisgeben will, kann einen Proxy-Server einschalten. Als Beispiele nannte sie Hotspot Shield und „CyberGhost“. „Das sind Vermittler“, verdeutlichte sie. Es ist quasi eine Umleitung über einen weiteren Server – statt direkt nach Schweden oder die USA geht es über einen Zwischenstopp beispielsweise in Island. „So

wird es schwierig, die IP-Adresse nachzuvollziehen“, erklärte sie das Prinzip. Wer beispielsweise eine US-Serie anschauen will, die nicht in Deutschland läuft, kann das über den Proxy-Server. „Das ist legal“, stellte sie klar. Die Proxy-Dienste muss sich der Nutzer jedoch herunterladen.

Vor WLAN warnte sie bei sensiblen Daten. In dem öffentlichen Netz sind die Daten unverschlüsselt. Es besteht dadurch die Gefahr, dass Kriminelle sie abgreifen können. „Wenn ich kurz über Facebook mit meiner Tochter kommuniziere, denke ich: Wen interessiert das, wenn ich mir gerade ein Eis gönne. Online-Banking würde ich aber nie machen“, nannte sie Beispiele. In Einkaufszentren wer-

de WLAN gerne angeboten. „Damit kann man sehen, wer wo und wie schnell durchgeht, vor einem Schaufenster stehen bleibt oder sich in einem Laden aufhält. Daraus ergeben sich dann Algorithmen“, so die Referentin.

Es gibt das Surface Net, das Deep Net und das Dark Net. „Surface Net – das ist alles, was wir nutzen. Im Deep Net sehe ich beispielsweise nicht nur den Bibliothekskatalog, sondern auch, was drin steht“, erläuterte sie den Unterschied. Das Dark Net ist so aufgebaut, dass niemand mehr in der virtuellen Welt zu finden ist. „Wir werden das aber nie nutzen. Es sind so viele Computer dazwischengeschaltet, dass alles sehr langsam läuft“, machte Jutta

Bundschuh klar. Sie nannte gleich mehrere Gefahrenquellen im Netz. Bei Phishing – Englisch für angeln – versuchen Kriminelle über gefälschte Webseiten oder Mails an persönliche Daten zu gelangen. „Pharming ist die Weiterentwicklung. Hier werden einem gefälschte Webseiten untergejubelt“, erklärte die Referentin. Trojaner installieren heimlich ein Schadprogramm und Keylogger überwachen oder rekonstruieren die Eingaben der Nutzer, um an vertrauliche Daten wie PINs zu kommen.

Die meisten Teilnehmerinnen haben immer wieder zum Kuli gegriffen und für sie relevante Themen mitgeschrieben. Auch Fragen waren erwünscht. Eine Zuhörerin wollte wissen, wie man einen PC am besten entsorgt. „Die Festplatte mit dem Hammer zertrümmern, bis er in Einzelteile zerfällt“, lautete der pragmatische Rat von Jutta Bundschuh.

Info Das digitale Erbe streifte die Referentin ebenfalls. Jeder sollte sich darum kümmern und einen digitalen Nachlassverwalter benennen, eventuell einen kommerzieller Anbieter. Die Übersicht sollte auf einem verschlüsselten oder mit einem Kennwort geschützten Datenträger wie USB-Stick gesichert sein, der im Tresor oder Bankschließfach sicher verwahrt ist. Darauf enthalten: die aktuelle Übersicht aller Accounts mit Benutzernamen oder Kennworten; Informationen darüber, welche Daten gelöscht werden sollen, was mit den Accounts in sozialen Netzwerken passiert, ebenso mit Fotos in den elektronischen Medien, einschließlich Cloud – und schließlich, was aus den Endgeräten samt den Daten geschehen soll.

Lesen, denken und dann erst klicken – Jutta Bundschuhs Tipps für Internetnutzer

„Mein wichtigster Tipp lautet: lesen, denken, klicken. – Was will derjenige von mir? Will ich das auch? Erst, wenn diese Fragen wirklich geklärt sind, klicke ich“, rät die Internet-Expertin Jutta Bundschuh eindringlich.

Große Vorsicht ist geboten, wenn einem etwas geschenkt wird. „Kostenlos ist selten was – es kostet einen die eigenen Dateien“, nennt sie den Grund für die Offerten. Jeder sollte sparsam mit der Verbreitung eigener Dateien umgehen und die Virencanner immer aktuell sein.

In soziale Netzwerke nicht unbedingt Bilder von sich oder Freunden und Familie stellen sowie die



eigene Adresse oder den Arbeitgeber nicht nennen.

„Das Google-Konto macht ganz gläsern. Es wird verfolgt, wo man hinget“, sagt Bundschuh. Deshalb dieses Konto überprüfen und anpassen. Mit dem Google Play-Store – damit kann man Apps, E-Books, Filme und mehr laden – können alle Suchanfragen verfolgt werden, ebenso ist ersichtlich, wo der Benutzer hinfährt oder -geht: „Bei den Einstellungen kann man es ausschalten.“

Nicht viel Geld ausgeben für die Geräte, denn sie werden schnell alt – spätestens, wenn das Nachfolgemodell auf dem Markt ist.

Empfohlene Seiten von Jutta Bundschuh bezüglich Sicherheit im Netz: www.sicher-im-netz.de www.bsi-fuer-buerger.de www.klickwafe.de www.silver-tipps.de

Kinderfreundliche Seiten sind ihrer Ansicht: www.internet-abc.de www.fragFINN.de www.blinde-kuh.de www.helles-koepfchen.de „Für Kinder ist es sinnvoll, mit diesen Seiten zu suchen. Sie sind kinderfreundlich, in verständlicher Sprache, und es finden sich nur Kinderthemen“, sagt Jutta Bundschuh. *ih*