Wintercamp: Sicher im Internet

Funktionsweise des Internets:
Im Internet hat jeder Computer eine IP-Adresse. Die beiden unterschiedlichen Arten von Computern im Internet sind die *Geräte der Benutzer* (z.B. Laptops, Handys) und die *Server* (bieten Dienste wie Websites an). Server sind immer angeschaltet und immer mit dem Internet verbunden, damit man jederzeit auf sie zugreifen kann. Sie stehen dicht beieinander in großen Hallen, die man Rechenzentren nennt. Wenn man im Internet einen Dienst benutzt, z.B. eine Website aufruft, dann wird die Anfrage in ein Paket gepackt und wie bei einem Postpaket mit Empfänger (die IP-Adresse des Routers) und Absender (die IP-Adresse des eigenen Gerätes) versehen. Damit das Paket vom Gerät zum Server kommt, wird es von vielen kleinen Computern, den *Routern*, weitergeleitet. Die größte Weiterleitungsstation in Deutschland, die auch Pakete in andere Länder weiterschickt, heißt DE-CIX und steht in Frankfurt. Das Internet hat sehr viele solcher Stationen, sodass es nicht schlimm ist, wenn mal Kabel oder Router ausfallen. Ein Paket nimmt sowieso selbst für das gleiche Ziel selten den gleichen Weg.

Verschlüsselung:
Der Inhalt der Pakete im Internet ist normalerweise leicht auslesbar. Es ist wie bei einer Postkarte, die jeder Postbote lesen könnte, nur dass wir im Internet viel wichtigere Dinge tun, als wir auf eine Postkarte schreiben. Deshalb ist es wichtig, dass die Programme, die man benutzt, verschlüsseln und damit den Inhalt schützen. Im Browser ist die Verschlüsselung aktiv, wenn in der Browserleiste die Adresse mit https:// beginnt. Mindestens überall, wo man sich einloggen kann, sollte man darauf achten dass dies der Fall ist. Man kann sich das *HTTPS Everywhere* Plugin (Firefox, Chrome oder Opera) installieren, welches sicherstellt dass immer wenn der Dienst verschlüsselt (https://...) und unverschlüsselt (http://...) zur Verfügung steht die verschlüsselte Variante genutzt wird. Die Websiteverschlüsselung (SSL bzw. TLS) ist eine *Transport- bzw. Wegverschlüsselung*, weil sie nur den Weg zum Server sichert, der Serveranbieter (z.B. Google) kann die Daten dann wieder auspacken und sieht den Inhalt. Wenn man direkt mit anderen Nutzern kommuniziert kann man auch die bessere *Ende-zu-Ende-Verschlüsselung* benutzen, die erst beim Empfänger aufgemacht werden kann und nicht schon vom Dienst. Nach diesem Prinzip funktioniert z.B. Email-Verschlüsselung (*GPG*) und diverse Messengerapps (z.B. *Signal oder ChatSecure*).

Metadaten:
Mit Verschlüsselung schützt man nur die Inhalte. Das reicht aber leider oft nicht, weil es für jede Kommunikation im Internet auch noch Metadaten gibt. Diese kann man mit den W-Fragen erfragen: Wer hat mit wem wie, wann und wo kommuniziert. Klassische Metadaten sind also die beteiligten Kommunikationspartner, der Ort an dem sie waren und wie sie miteinander in Verbindung getreten sind. Kommunikationspartner müssen dabei nicht unbedingt Menschen, sondern können auch Maschinen, z.B. Server, sein. Was für eine Website man ansurft ist also z.B. auch ein Metadatum. Viele Metadaten kann man leider nicht vermeiden. Deshalb ist es gesellschaftlich wichtig, dass der Staat keine Vorratsdatenspeicherung (bei der es um

Metadaten geht) macht, weil man mit vielen Metadaten mehr über eine Person herausfinden kann, als mit den Inhalten. Viele solche Daten zusammen ergeben nämlich ein *Persönlichkeitsprofil*, das mehr über einen aussagen kann, als es der beste Freund könnte. Ein paar Metadaten kann man allerdings doch recht einfach loswerden. Mit den Plugins *Privacy Badger* (Firefox, Chrome) oder *Disconnect* (Firefox, Chrome, Safari, Opera) kann man verhindern, dass Werbefirmen im Internet sehen können, welche Websites man sich angeguckt hat.

Verhalten im Internet und in sozialen Netzwerken

Wenn man im Internet etwas öffentlich schreibt, dann kann es jeder lesen. Informationen, die einmal offen im Internet waren, bekommt man auch nie wieder gelöscht. Mindestens genau so wichtig, wie sich Gedanken über seine eigenen Daten zu machen ist es, nicht die Daten anderer Leute (z.B. Fotos) ins Internet zu stellen ohne sie gefragt zu haben. Um seine eigenen Daten und Zugänge zu schützen, ist es sehr wichtig, sichere Passwörter zu benutzen. Sie sollten lang sein und viele unterschiedliche Zeichen (Kleinbuchstaben, Großbuchstaben, Zahlen, Sonderzeichen) beinhalten. Es ist wichtig, dass man mindestens für sein Emailkonto ein Passwort benutzt, dass man nirgendwo anders verwendet.