Presseinformationen für Gemeinden
Unser monatlicher Tipp für Ihre Gemeinde!

Thomas Hauser, Landesgeschäftsführer und Pressesprecher
02272/61820 28, thomas.hauser@noezsv.at

Mit dem Internet „auf Du“

Es gibt heute kaum jemanden, dem der Begriff „Internet“ nichts sagt. Immerhin hat der erste Vorläufer des heutigen Internet schon im Jahr 1969 gestartet – damals hat dieses „Internet“ aber lediglich vier Forschungseinrichtungen vernetzt. Das Internet hat in den letzten Jahrzehnten unser Leben grundlegend geändert. Und genauso grundlegend hat sich auch die Sicherheit im „World Wide Web“ verändert und wir müssen uns mit den Gefahren auseinandersetzen.

Das Internet hat die Welt in den vergangenen Jahren fundamental verändert. In Ländern wie dem Iran, in China oder in Ägypten wurde und wird es von Oppositionellen im Kampf um mehr Freiheit genutzt. E-Mail, Instant Messaging und kostenlose Videotelefonie verkürzen heute die Distanzen zwischen um den Erdball verstreuten Freunden oder Familienangehören. Es ist eine globale Kultur des Teilens und Zusammenarbeitens entstanden, deren eindrucksvollstes Ergebnis sicher „Wikipedia“ heißt – wer hätte vor 20 Jahren geglaubt, dass ganz normale Menschen einmal gemeinsam (!) und unentgeltlich (!) eine immens wertvolle Ressource schaffen würden, die nun vom ganzen Planeten genutzt werden kann?

Gleichzeitig hat das Internet aber auch Gefahren gebracht, Abscheulichkeiten verfügbar gemacht und dem Terror und dem Wahnsinn völlig neue Vernetzungs- und Organisationsmöglichkeiten eröffnet. Insgesamt aber ist das Internet eine Vereinfachung für unser Leben. Und das Netz ist vor allem eins: Der größte Informationsvermittler und -speicher, den die Menschheit jemals zur Verfügung hatte. Es ist noch nicht allzu lange her, dass in Europa noch Konsens darüber herrschte, dass mehr Information in der Regel besser ist als weniger Information. Dass die Möglichkeit, Bildung und Wissen zu erwerben, begrüßenswert ist, dass die Welt dadurch zu einem besseren, freieren, womöglich glücklicheren Ort wird.

Manchmal kann man heutzutage den Eindruck bekommen, dieser alte Konsens gelte nun nicht mehr: Weil unter der vielen Information im Netz auch so viel ist, das dem einen oder anderen nicht behagt. Und die vielen kriminellen Subjekte, die das WWW für ihre eigenen Zwecke und zur persönlichen Bereicherung benützen. Hier heißt es „Augen offen halten“ und jede Information oder jedes (zu-gute?) Angebot zumindest kritisch zu hinterfragen. Schauen Sie sich zunächst mal die Vor- und Nachteile genauer an:

Die Vorteile des Internet:

- Schnelle Verfügbarkeit des nationalen und internationalen (Informations-)Angebots
- Anonymität
- Bequemlichkeit, Benutzerfreundlichkeit
- Geschwindigkeit des Mediums
- Aktualität (Aktualisierung von Informationen sehr rasch und einfach möglich)
- Kostenersparnis
- Zeitliche Unabhängigkeit (24 Stunden erreichbar)
- Globale Kommunikation
- Große Verbreitung
- Möglichkeit des Informationsaustausches
- Grafische Benutzeroberfläche

Die Nachteile des Internet:

- Datenschutz, Sicherheitsproblematik
- Kurzlebigkeit (z.B. von Informationen oder Webseiten)
- Fruchtbarer Boden für illegale Geschäfte aufgrund mangelnder Rechtslage
- Qualität der Informationen?
- „Spurenhinterlassen“ >> Werbezusendungen, Sicherheit
- Virenprogramme, Hacker...
- Teilweise noch fehlende Akzeptanz des Mediums?
- Voraussetzung für effektiven Gebrauch: Grundwissen über den Umgang mit dem Internet und Kenntnis effizienter Suchstrategien >> ansonsten hoher Zeitaufwand und Frustrationserlebnisse
- Technisches Grund – Know-How ist notwendig

Quelle: Universität Wien (homepage.univie.ac.at)

In der heutigen, schnelllebigen Zeit ist das Internet wohl kaum aus dem täglichen Leben wegzudenken, daher kann wohl die Behauptung aufgestellt werden, dass die Vorteile des Internet die Nachteile überwiegen. Aber auch gerade deswegen sollte niemand ohne entsprechende Sicherheitsvorkehrungen im World Wide Web „surfen“.
Die Virenjäger der deutschen Firma „Avira“ haben zum Safer Internet Day 2016 zehn Gebote zusammen-gestellt, mit denen Nutzer ihren PC gegen unerwünschte Eindringlinge absichern und ihre wertvollen Daten vor unbefugtem Zugriff schützen können. Hier sind Aviras zehn Gold-Tipps für mehr Sicherheit am PC, aber auch am Smartphone:

1. Niemals ohne Virenschutz!

Egal, ob am PC oder am Smartphone: Ein Virenscanner sollte auf keinem Gerät fehlen, das sensible Daten enthält. Weil es sowohl für den PC, als auch für Android-Handys taugliche Virenscanner zum Nulltarif gibt, ist das auch kein Problem. Tipp: Um den besten Virenschutz für Ihre Bedürfnisse zu finden, lohnt sich ein Blick auf Vergleichsportale wie „AV-Test“ oder „ComputerBild“.

2. Aktualisieren Sie Ihre Software!

Fehlerfreie Software gibt es nicht. Egal, ob Betriebssystem, Hilfs-Software, Treiber oder Multimedia-Tools à la Adobe Flash: Alle Programme, die Sie verwenden, sollten stets auf dem aktuellen Stand sein. Deshalb sollten Sie Update-Benachrichtigungen nicht einfach wegklicken, sondern auf die Aktualität Ihrer Software achten. Im Zweifel tut ein Update nämlich weit weniger weh als ein Virus, der es über eine nicht gepatchte Sicherheitslücke auf Ihr Gerät schafft.

3. Seien Sie geduldig!

Virenscanner haben eine unangenehme Eigenschaft: Sie bremsen das System – manche mehr, manche weniger. Das liegt daran, dass Sicherheitssoftware im Hintergrund gerne nach verdächtigen Aktivitäten sucht. Auch, wenn Ihr PC dadurch etwas langsamer ist, sollten Sie die Scans nicht abbrechen, da Sie sonst den Schutz des Systems gefährden. Wenn Sie der Virenscan trotzdem nervt, ist es ratsam, ihn während der Nachtstunden erledigen zu lassen. Im Virenscanner kann man den Zeitplan üblicherweise einstellen.

4. Ihr Konto sollte nicht alles dürfen!

Ein Administratorkonto am PC ist bequem, aber auch gefährlich. Erlangt ein Angreifer Zugriff, kann er damit viel Schaden anrichten. Es ist deshalb empfehlenswert, wenn Sie auf Ihrem PC nicht alles mit dem Administratorkonto erledigen, sondern bei der alltäglichen Nutzung mit eingeschränkten Rechten arbeiten und das Admin-Konto nur dann benutzen, wenn Sie es brauchen. Das reduziert die Wahrscheinlichkeit, dass Viren Änderungen an Ihrem System durchführen können.

5. Klicken Sie nicht auf jede Reklame!

Werbung ist im Netz omnipräsent, kann aber auch zur Lieferung von Adware (ein Kofferwort aus engl. Advertisement (dt.: „Reklame“, „Werbung“) und Software. Es bezeichnet Software, die dem Benutzer zusätzlich zur eigentlichen Funktion Werbung zeigt bzw. weitere Software installiert, welche Werbung anzeigt) oder für Phishing-Angriffe missbraucht werden. Deshalb gilt: Lassen Sie bei Klicks auf Werbung Vorsicht walten und machen Sie einen Bogen um dubiose Websites. Es gibt auch technische Hilfsmittel, die gefährliche Anzeigen identifizieren.

6. Verschlüsseln Sie Ihre Kommunikation!

Gerade bei Nutzung fremder WLAN-Netzwerke – etwa im Kaffeehaus – sollten Sie Daten nie unverschlüsselt übertragen, man weiß schließlich nie, wer mitliest. Beim Surfen empfiehlt sich deshalb die Nutzung des verschlüsselten HTTPS-Standards. Weil der aber nicht von jeder Website automatisch genutzt wird, ist die Verwendung eines Browser-Add-Ons wie „HTTPS Everywhere" ratsam. Damit zwingen Sie den Server, verschlüsselt mit Ihnen zu kommunizieren. Noch sicherer, aber nicht zwangsläufig gratis: ein VPN-Tunnel sichert nicht nur den Surf-, sondern Ihren kompletten Datenverkehr ab.

7. Nutzen Sie sichere Passwörter!

Schützen Sie Ihre Konten mit einem starken Passwort, also nicht mit „123456". Als sicher gelten längere Kombinationen aus Buchstaben, Zahlen und Sonderzeichen oder ein mit Sonderzeichen wie einem Binde-strich getrennter Satz. Verzichten Sie darauf, das gleiche Passwort für mehrere Websites zu verwenden. Damit Sie sich komplexere Passwörter nicht merken müssen, bietet sich ein Passwort-Manager wie „KeePass" an. Ebenfalls eine gute Idee: Viele Websites bieten heute Zwei-Faktor-Authentifizierung an, bei der zusätzlich zum Passwort das Mobilgerät des Nutzers als Erkennungsmerkmal genutzt wird.

8. Entfernen Sie Sicherheits-Altlasten!

Nicht mehr verwendete Internet-Anwendungen, die womöglich auch nicht mehr aktuell gehalten werden, sind ein Sicherheitsrisiko. Löschen Sie diese von Ihrem PC. Zwei Beispiele für solche Tools sind etwa Flash und Java. Sie werden heute nur mehr von wenigen Websites gebraucht, sind aber immer noch auf den meisten PCs installiert – inklusive teils schwerer Sicherheitslücken.

9. Seien Sie geizig bei Ihren Daten!

Große Internetkonzerne wie Google oder Facebook verdienen mit dem Sammeln und der Auswertung von Nutzerdaten Milliarden. Wenn Ihnen das suspekt ist, können Sie der Datensammelei einen Riegel vorschieben und der Schnüffelei mit Tools wie dem Browser-Add-On „Ghostery" ein Ende machen.

10. Seien Sie immer misstrauisch!

Die besten Sicherheitstipps helfen nichts, wenn der Anwender leichtfertig E-Mail-Anhänge aus dubiosen Quellen öffnet oder dem vermeintlichen Microsoft-Techniker am Telefon seine Passwörter verrät. Auch auf Phishing-Ganoven, die mit gefälschten Mails auf Nutzerfang gehen, fallen immer noch viele Computernutzer herein. Deshalb gilt als oberste Regel: Seien Sie immer misstrauisch, hinterfragen Sie dubiose Angebote und klicken Sie nicht auf verdächtige Links oder Anhänge in (möglicherweise) gefälschten E-Mails!

Quelle: krone.at, 9. Februar 2016

Und ans Herz gelegt sei allen Internet-Usern auch die Seite www.sicher-im-internet.at .

HAUSER Thomas
Landesgeschäftsführer
Niederösterreichischer Zivilschutzverband
Langenlebarnerstrasse 106
3430 Tulln
02272/61820 28
02272/9005 13198
0664 8444489
thomas.hauser@noezsv.at