Vorwort

Die Sicherheit am Computer und Smartphone wird immer wieder in der Öffentlichkeit diskutiert. Auch die Presse und der Rundfunk berichten zunehmend häufiger über Virenattacken, Hackerangriffe und fragwürdiger Informationsbeschaffung. Wir haben den Eindruck, dass viele Anwender resigniert haben und Sicherheitsrisiken eher in Kauf nehmen als etwas dagegen tun zu wollen. Dabei gibt es einfache Möglichkeiten der Vorbeugung. Wir möchten Ihnen hier grundlegende und einfach umzusetzende Verhaltensweisen und Abwehrstrategien vorstellen, die zumindest das Surfen und Mailen betreffen.

Es ist relativ einfach, Programme unter Windows zu installieren. Deren Benutzer sind sehr schnell dabei, insbesondere kostenfreie Testsoftware, Spiele und freie Programme zu installieren. Auch günstige Hardware ist schnell eingerichtet, genauso vermeintlich bessere Treibersoftware. Und das ist überwiegend das Problem.

Wie kann der Windows-Anwender gegensteuern?

Die Programme und Treiber werden unkritisch und meist ohne zu überlegen, welcher Herkunft sie sind, installiert! Im besten Fall zeigt die installierte Anwendung keinen negativen Einfluss, im anderen Fall führt sie zur Instabilität von Windows und im schlechtesten Fall hat der Anwender eine Manipulationssoftware oder einen Virus auf das System übertragen, ohne dass der Antivirenscanner einen Alarm ausgelöst hat.

Ein Virenscanner kann aktuelle Bedrohungen nur mit einem gewissen Zeitversatz erkennen und bekämpfen. Es wird also immer zuerst Opfer einer Attacke geben, bevor die Hersteller von Schutzsoftware darauf reagieren können. Wie schnell sie dazu Imstande sind, zeichnet die Güte des Abwehrprogramms aus!

Regel 1: *Bevor Sie also etwas installieren, sollten Sie sich zuerst entweder über die konkrete Software im Internet informieren, z.B. über die Google Suche oder Ihren Fachhändler vor Ort befragen.*

Sind Updates für Windows Systeme wichtig?

Windows Updates und auch die Aktualisierungen von Anwendungen, Geräten (Firmware) und Herstellertreibern sollen nicht nur das bestehende System verbessern, sondern schließen in vielfachen Fällen sogenannte Sicherheitslücken. Diese bestehen darin, dass ein Entwickler Möglichkeiten für Hacker übersehen hat, in ein System unbefugt einzudringen. Insofern tragen Updates wesentlich zur Sicherheit, aber auch Laufstabilität des Gesamtsystems bei!

Regel 2: *Regelmäßig Windows Updates durchführen und kontrollieren, ob Updates bereitgestellt sind.*

Das Windows Update finden Sie unter *Start - PC-Einstellungen - Update und Sicherheit.*

Zuweilen kann es jedoch - wenn auch selten - vorkommen, dass ein Update das System auf irgendeine Weise beeinträchtigt. Dennoch sollten Sie immer updaten, da die Vorteile einen solchen Nachteil übertrumpfen. Außerdem können Sie ein Update auch unmittelbar nach Installation leicht deinstallieren. (*Start - PC-Einstellungen - Update und Sicherheit – Updateverlauf anzeigen – Updates deinstallieren*)

Vielen Anwendern ist das Updaten lästig! Sie wollen damit keine Zeit verbringen. Soll sich doch der PC darum selbst kümmern. Ein Computer ist jedoch nichts anderes als ein modernes Werkzeug,

welches auch gepflegt werden muss. Lassen Sie Ihren Hammer nach getaner Arbeit draußen bei Regen und Nässe so einfach liegen? Dann ist es nur noch eine Frage der Zeit bis Sie ihn für die gedachten Einsatzzwecke nicht mehr nutzen können. Denken Sie über den Vergleich nach!

Webseitenabruf

Häufig geben Internetanwender auch Ihnen bekannte Internetseiten über ein Suchfeld Ihres Browsers ein statt die vollständige Internetadresse in der Adresszeile des Browsers einzutragen oder über Favoriten (Internet Explorer) bzw. Lesezeichen (Mozilla Firefox und andere) dort abzuspeichern und fortan abzurufen. Sie laufen damit Gefahr, auf eine Internetseite zu gelangen, wo Sie eigentlich nicht hin wollten. Z.B. geben Sie infolge eines Schreibfehlers "sparkase.de" statt "sparkasse.de" ein, gelangen Sie möglicherweise auf eine gefälschte Internetseite Ihrer Sparkasse oder eine Seite mit einem Virus wartet auf der vermeintlichen Zielseite auf Sie. In jedem Fall haben Sie dort nichts Gutes zu erwarten! In vielen Fällen wird eine eingesetzte gute Suchmaschine dies jedoch zu verhindern wissen und / oder Ihnen eine korrekte Seite vorschlagen!

Es ist auf jeden Fall cleverer, wichtige Internetseiten unter den Favoriten bzw. Lesezeichen abzuspeichern und bei Bedarf abzurufen. Auch ist es ratsam, bei Suchmaschinen die Liste mit Suchergebnissen in der Vorschau auf Ihren Inhalt zu untersuchen. Sind Sie wirklich mit einem Klick auf der gesuchten Firmenseite? Der erst beste Eintrag ist es meistens nicht!

Regel 3: *Rufen Sie Ihnen bekannte Webseiten nur über die Adresszeile bzw. Lesezeichen oder Favoriten Ihres Browsers auf.*

Regel 4: *Beachten Sie bei Einsatz einer Suchmaschine deren Ergebnisvorschlagseinträge und wählen Sie den richtigen aus!*

E-Mailverkehr

Auch E-Mails bergen die Gefahr, dass in den dargestellten Bildern und Links ein Virus auf Sie wartet. Manche sind so geschickt aufgebaut, dass Sie denken könnten, das Schreiben kommt von Ihrem bevorzugtem Internethändler, Ihrer Bank oder einem Ihnen bekannten Kontakt. Meist finden Sie aber Unstimmigkeiten, auf die man zuerst einmal nicht geachtet hat. Schärfen Sie deshalb Ihre Augen und öffnen Sie die E-Mail nicht ohne weiteres. Das Vorschaufenster reicht zur Entlarvung einer Fälschung, indem Sie Sprache, Adressdaten, Bankverbindung und Schreibstil beachten. Vor allem Unternehmen schreiben Ihnen in perfektem Deutsch. Sie achten nämlich auf Schreib- und Grammatikfehler und

sind von den "Scheinunternehmern" leicht zu unterscheiden. Bewerten Sie vor allem, ob alle Angaben stimmig sind! Ansonsten löschen Sie die E-Mail. Neugierde kann hier nur schaden!

Regel 5: *Klicken Sie bei E-Mails nicht unbedacht Links, Bilder oder Anhänge an. Achten Sie auf Plausibilität von Informationen*

Perfekter Schutz und Sicherheit?

In den aufgeführten Fällen kann Sie ein guter Viren- und Schadsoftwarescanner (engl. Malware) im Regelfall schützen und für ausreichende Sicherheit sorgen. Wir empfehlen die Vollversion von Malwarebytes. Doch jeder auch noch so gute Virenscanner kann Falschalarme auslösen oder einfach im konkreten Fall versagen. Den perfekten Schutz können Sie leider nicht kaufen! Ein gutes Abwehrprogramm, Ihr gesunder Menschenverstand und Ihre Aufmerksamkeit können Sie jedoch schon äußerst effektiv vor den Gefahren aus dem Internet schützen.

Ein letzter Tip: Das Windows Betriebssystem unterscheidet zwischen Standardbenutzern und Administratoren. Nur Letztere dürfen Anwendungen installieren! Legen Sie deshalb ein oder mehr Administratoren mit sicherem Passwort an. Diese loggen sich nur ein, um administrative Aufgaben zu erfüllen. Die anderen Benutzer sollten als Standardbenutzer den PC zur Arbeit nutzen, z.B. Surfen und Mailen oder Programme ausführen. Über diese Logik kann sich auch ein Virus nur schwer verbreiten. Windows fragt nämlich immer einen Administrator, ob Veränderungen am System durchgeführt werden sollen. Ohne zugehöriges Passwort und Bejahung der Frage wird beim Standardbenutzer keine Aktualisierung bzw. Installation durchgeführt.