Sicherheit am PC

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 Verhaltensweisen und Abwehrstrategien verdeutlichen, die zumindest das Surfen und Mailen betreffen. Natürlich sprechen wir auch unsere Dienstleistungen im Bereich an. Dies betrifft Risiken bei der Hausautomation und Fernzugriff oder die Implementierung von erweiterten Sicherheitsstrategien mit Hardwareeinsatz. Zu Gunsten unserer Aufklärungsabsicht sind diese Themen relativ kurz gefasst.

PCs bzw. Windows Betriebssysteme haben den Ruf, sehr unsicher bezüglich Hackerangriffe und Virenbefalls zu sein. Dazu ist zu sagen, dass PCs mit den Microsoft Betriebssystemen aufgrund des weiten Verbreitungsgrades tatsächlich die meist angegriffenen und folglich auch betroffenen Systeme sind.

Die Ursachen für die Virenanfälligkeit

Ein wesentlicher Unterschied zu anderen Betriebssystemen liegt in der Tatsache, dass die Firma Microsoft die Bedienungsfreundlichkeit und Erweiterbarkeit im Hard- und Softwarebereich bei der Entwicklung in den Vordergrund gestellt hat. Es gibt wohl kaum ein System, dass eine so breite und differenzierte Basis von Geräten und Treibern unterschiedlichster Leistungsfähigkeit unterstüzt. Auch gibt es jede Menge an Software – von freien kostenlosen bishin zur professionellen und kostenpflichtigen Angeboten.

Andere und zum großen Teil nachfolgende Betriebssystementwickler haben aus diesem “Fehler” von Microsoft gelernt und ihr Augenmerk auf die Sicherheit gelegt, haben aber auch zugleich die Erweiterungsmöglichkeiten ihres Systems beschnitten. Linux verfügt über meist generische Treiber für leistungsmäßig unterschiedlichste Hardware und eine beschränkte Softwareauswahl. Der Bedienungskomfort stand anfangs nicht im Vordergrund. Apple setzte auf überschaubare Hard- und Softwareangebote, also Homogenität wie auch auf Bedienungskomfort. Beide zuletzt genannten Betriebssysteme sind relativ robust gegen Hackerangriffe, wenn auch Apple diesbezüglich im August 2022 öffentlich gegenüber ihrer stetig wachsenden Kundschaft gravierende Sicherheitsmängel in Ihren Betriebssystemen eingestehen musste. Notwendigerweise schaffte das Unternehmen Abhilfe durch Sicherheitsupdates sowohl für iMACs wie auch für iPhones und iPads. Willkommen im Club häufig genutzter Betriebssysteme!

Die Android-Systeme von Google spielen im PC-Bereich derzeit kaum eine Rolle. Das liegt vor allem an der fehlenden Flexibilität bezüglich der Einsatzfähigkeit von bekannten Anwendungen. Sie kommen nicht über die Nutzungsebene und Funktionen eines Smartphones hinaus. Android soll bezüglich der Sicherheit laut der Computerfachzeitschrift CHIP sehr anfällig sein.

Linux bzw. seine verschiedenen Distributionen sind hardwaremäßig relativ anspruchslos und im Privatbereich kostenfrei einsetzbar. Apple ist hingegen extrem teuer. Androidsysteme sind in der Regel sehr preisgünstig und bei Microsoft Systemen ist für jeden Geldbeutel etwas dabei.

Wo kann der Windows-Anwender gegensteuern?

Da es so einfach ist, Windowsprogramme zu installieren, sind dessen Benutzer sehr schnell dabei, insbesondere kostenfreie Testsoftware, Spiele und freie Programme zu installieren. Auch günstige Hardware ist schnell eingerichtet. Und das ist überwiegend das Problem!

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!

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 Treibern 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 und Laufstabilität des Gesamtsystems bei!

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!

Webseiten- und Emailverkehr

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) abzurufen. Sie laufen damit Gefahr, auf eine Internetseite zu gelangen, wo Sie eigentlich nicht hin wollten. Z.B. geben Sie “Sparkase” 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, 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 meist nicht!

Auch Emails 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. 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!

Perfekter Schutz und Sicherheit?

In den aufgeführten Fällen kann Sie ein guter Viren- und Schadsoftwarescanner (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 am Computer 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. Nur 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 keine Aktualisierung bzw. Installation durchgeführt.

Erweiterte Sicherheit

Falls Sie Heimarbeitsplätze oder einen Fernzugriff auf Ihren PC planen oder auf Geräte einer Hausautomation zugreifen wollen (z.B. Kameras, Heizungssteuerung und dergleichen), sollten zusätzliche Sicherheitsmaßnahmen umgesetzt werden. Dies betrifft auch die eingesetzte Firewall. Gerade in Betrieben mit regem Internetverkehr ist der Einsatz von Sicherheitsstrategien zu empfehlen. Dazu zählen Schulungsmaßnahmen für die Mitarbeiter genauso dazu wie der Einsatz von Scriptblockern, Schutzsoftware und -geräten wie Proxies, Emailservern und Hardwarefirewalls zum Schutz von Kundendaten und der Arbeitssysteme. Bei Bedarf nehmen Sie bitte mit uns Kontakt auf. Weitere Fragen zur Thematik der Sicherheit am Computer können wir Ihnen jederzeit beantworten. Wir beraten Sie gerne und qualifiziert!

Besuchen Sie auch unsere Serviceseite Tips & Tricks, auf der wir demnächst nicht nur Artikel zur Sicherheit veröffentlichen, sondern ganz allgemein nützliche Ratschläge und Empfehlungen zum Umgang mit dem PC und Programmen bereitstellen.

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.