Goldene Regeln für Computersicherheit

SPD
Parteivorstand

10.07.17

Goldene Regeln für Computersicherheit

Betriebssystem, CMS und Anwendersoftware auf dem aktuellen Stand halten

Betriebssysteme, CMS und Anwendungen weisen immer wieder Schwachstellen auf, die die Sicherheit deines Computers gefährden. Installiere regelmäßig die "Sicherheits-Updates", "Patches" und "Service Packs" der Hersteller, um Schwachstellen zu beseitigen.
Sicher ist: Besser rechtzeitig die Software aktualisieren, als alles neu installieren zu müssen!

Installation und Nutzung von zusätzlicher (privater) Software

Mit jeder neuen Softwarekomponente steigt der Verwaltungsaufwand und das Sicherheitsrisiko. Insbesondere kostenfreie Software die man frei über das Internet beziehen kann (Download) beinhaltet häufig Malware-Komponenten, enthält Sicherheitslücken und kann auch Schadprogramme enthalten. Deshalb installiere nur Software, die aus sicheren Quellen stammt, zweifelsfrei richtig lizenziert ist und auch tatsächlich für die Tätigkeit regelmäßig benötigt wird. Suche im Zweifelsfall den Rat erfahrener Anwender oder Systemadministratoren

Aktuelle Virenscanner benutzen

Ein professioneller und aktueller Virenscanner gehört zum Basisschutz eines jeden Computers. Achte darauf, dass dieser aktiviert ist und auf dem aktuellen Stand gehalten wird. Sicher ist: Virenschutz ist Basisschutz, kein Luxus! Gute Virenscanner kosten regelmäßig auch Geld, denn sie erfordern eine dauerhafte und intensive Beschäftigung mit vorhandenen und neu entwickelten Schadprogrammen. Bei kostenlosen Virenscannern muss man häufig Abstriche bei der Aktualität und den Schutzmechanismen in Kauf nehmen.

Firewall bei Computern verwenden, die mit dem Internet verbunden sind

Eine Firewall schützt den Computer vor unberechtigten Zugriffen aus dem Internet bzw. aus dem Netzwerk, an das er angeschlossen ist. Wenn du mit deinem Computer im Internet oder einem Netzwerk arbeitest, stelle sicher, dass die lokale Firewall installiert und aktiviert ist. Aktuelle Betriebssysteme (Windows, Linux, Mac OS X) bieten bereits eine integrierte Firewall für einen Basisschutz an. Sicher ist deshalb: Niemals ohne Firewall ins Netz!

Sichere Passwörter verwenden und sicher speichern

Einfache und kurze Passworte sind leicht zu merken. Aber sie sind nicht sicher.
Nutze minimal acht Zeichen mit einer Kombination aus mindestens drei der vier folgenden Zeichengruppen: Ziffern Großbuchstaben, Kleinbuchstaben, und Sonderzeichen.
Verwende keine Trivialpassworte wie Namen, Geburtstage oder Wörter, die in Wörterbüchern stehen.
Benutze für unterschiedlich Anwendungen und Bereiche auch unterschiedliche Passwörter.
Behandle deine Passwörter wie die PIN deiner Bankkarten. Gib Sie nicht weiter, auch nicht, wenn du von vermeintlich vertrauenswürdigen Personen oder Stellen dazu aufgefordert wirst.
Notieren deine Passwörter niemals sichtbar, wechsle Sie regelmäßig (mind. halbjährlich) und speichere Sie, wenn überhaupt, nur geschützt auf dem Computer, besser noch auf einem

Zweitgerät ab. Nutze dazu am besten bewährte Passwort-Tresore wie beispielsweise KeePass oder PasswordSafe.

Nutze am besten Passwort-Phrasen, um dir sichere Passwörter einfach zu merken:
Die **S**PD **g**ewinnt **d**ie **B**undes**t**ags**w**ahl 2017**!** → DSgdBtw2!

Möglichst nicht mit Administratorrechten auf dem Computer arbeiten

Wenn du mit Administratorrechten auf deinem Computer arbeitest, haben auch Schadprogramme uneingeschränkten Zugriff auf das System und können erst so ihre volle Wirkung zu entfalten. Deshalb lege auf deinem Computer immer zwei Konten an, ein Benutzerkonto mit eingeschränkten Rechten und ein Administratorkonto für die Verwaltung des Computers. Arbeite im Alltag nur mit dem Benutzerkonto mit eingeschränkten Rechten. Administratorrechte sind nur notwendig, um z.B. Änderungen an der Konfiguration vorzunehmen oder Software zu installieren.

Vorsicht bei unbekannten oder unerwarteten Dateianhängen an E-Mails

Eine große Anzahl von "Malware" (schädliche Software wie Viren, Würmer, Trojaner oder Verschlüsselungs- (Ransom-) Software) verbreitet sich per E-Mail oder über eingebettete Links. Öffne deshalb niemals leichtfertig E-Mail-Anhänge oder Links, die du nicht kennst oder nicht erwartest. Jeder Anhang, jeder Link, den du öffnest, egal, wie vertrauenswürdig er erscheint, kann die Sicherheit deines Computers gefährden. Auch Absender, die du kennst, können (unwissentlich) E-Mails mit Schadsoftsoftware verschicken! Absenderinformationen lassen sich auch fälschen! Im Zweifel kannst du zur Sicherheit telefonisch nachfragen, auch wenn das von einigen belächelt wird.
Sicher ist aber: E-Mail-Anhänge und Links besser einmal zu wenig, als einmal zu viel öffnen!

Aufpassen beim Surfen im Internet

Auch beim Surfen im Internet lauern Gefahren. Manche Abzock-Site tarnt sich als Routenplaner und nicht selten versucht eine Site, die vor Sicherheitslücken warnt, einen Trojaner auf deinem Computer zu installieren. Deshalb gilt vor allem auf Internetseiten, die du nicht kennst:
Bevor du auf einen Link klickst, schau dir genau an, ob du auch wirklich die Seite aufrufen möchtest, die sich dahinter verbirgt. In der Fußzeile des Browsers siehst du meist, wohin der Link führt. Besondere Vorsicht ist bei Download-Links geboten. Öffne niemals eine Datei direkt, sondern speichere sie vor dem Öffnen immer erst auf deiner lokalen Festplatte. Dann hat dein Virenscanner eine größere Chance, ein eventuelles Schadprogramm zu erkennen, bevor der Schaden eingetreten ist.
Vorsicht bei Bezahldiensten und Treuhandservices. Prüfe immer vorher, ob der Dienst bekannt und seriös ist.
Achte auch darauf, dass du immer die aktuellste Version deines Browsers benutzt und verfolge die Meldungen, die es häufig zu Sicherheitslücken bei Browsern gibt.

Regelmäßige Datensicherung

Eine regelmäßige Sicherung (Backup) deiner wichtigen Daten schützt diese vor Verlust. Die meisten Betriebssysteme (Windows, Linux, Mac OS X) bieten bereits integrierte Funktionen für eine einfache Datensicherung an. Besonders bei den in der jüngsten Vergangenheit häufig

auftretenden Verschlüsselungs- (Ransom-) Angriffen ist eine regelmäßige Datensicherung der sicherste Schutz. Sind die Daten erst einmal verloren und nicht wieder herstellbar, kann es sehr schnell sehr teuer und zeitaufwendig werden.
Sicher ist deshalb: Sichere deine wichtigen Daten rechtzeitig und regelmäßig!

Datenschutz mit Verschlüsselung sensibler Daten

Sichere deine vertraulichen Daten und die Daten anderer gegen einen unberechtigten Zugriff durch Dritte indem du sie verschlüsselst. Aktuelle Betriebssysteme (Windows, Linux, Mac OS X) bieten dazu bereits einfache Mechanismen an. Alternativ kann auch kostenlose und quelloffene Software wie beispielsweise Truecrypt oder Veracrypt genutzt werden. Vergiss im Gegenzug aber nicht die Passwörter für verschlüsselte Daten sicher zu hinterlegen. Gehen diese verloren, sind die Daten für dich nicht mehr nutzbar. Nutze auch bei der Kommunikation mit sensiblen Daten Verschlüsselungsmöglichkeiten. Eine unverschlüsselte E-Mail ist wie eine Postkarte. Jeder, der es darauf anlegt, kann sie mit geringem Aufwand mitlesen.

Nutzung von Cloud-Diensten

Die Nutzung von Cloud-Services bietet unter anderem die Möglichkeit, Daten unabhängig von deinem lokalen Computerspeicher gleichzeitig an mehreren Orten, mit anderen Computern und auch mit anderen Menschen zu benutzen. Dies hat zweifellos Vorteile, birgt aber auch vielfältige Sicherheitsprobleme. Bei der Auswahl des geeigneten Cloud-Anbieters ist zum Beispiel dem Datenschutz eine hohe Priorität einzuräumen. Werden personenbezogene Daten außerhalb des Geltungsbereiches des deutschen bzw. europäischen Datenschutzrechtes gespeichert, kann ein Verstoß gegen das Datenschutzrecht vorliegen. Die Verantwortung dafür trägt aber nicht der Cloudanbieter, sondern der Nutzer des Dienstes.

Auch bei sensiblen Daten ist Vorsicht geboten. Vor der Nutzung muss zum Beispiel sichergestellt sein, dass die Daten nicht durch unbefugte Dritte benutzt werden können, eine verschlüsselte Übertragung möglich ist, die Daten regelmäßig gesichert werden, eine hohe Verfügbarkeit für berechtigte Nutzer gewährleistet ist und dass sämtliche Daten bei Vertragsauflösung mit dem Cloudanbieter rückstandslos gelöscht werden können. Kostenlose Accounts der großen Anbieter (Google, Dropbox, Microsoft, usw.) sind im Zusammenhang mit sensiblen und sicherheitsrelevanten Daten keine gute Lösung und verstoßen bei Nutzung durch Firmen und Institutionen möglicherweise auch gegen geltendes Recht. Als Alternative zu Cloudanbietern bietet sich eine eigene Cloud an. Anbieter für ein kostengünstiges NAS ist z.B. Synology mit seinen Diskstations.

Aufmerksam, kritisch und informiert bleiben

Sicherheit ist kein Produkt, das man kaufen, installieren und vergessen kann. Ein aktuelles System mit Virenscanner und Firewall bietet nur einen technischen Basisschutz.
Bleibe deshalb aufmerksam, kritisch und informiert, wenn es um die Sicherheit deines Computers geht. Gedankenlosigkeit oder Vertrauensseligkeit hebeln jeden technischen Schutz aus. Egal ob jemand bösartige Software auf deinem Computer installieren will, es auf wichtige Daten oder das Geld auf deinem Konto abgesehen hat. Er wird mit allen Tricks versuchen, sein Ziel zu erreichen. Nur wenn du aufmerksam bist, kannst du das verhindern. Ein gut geschützter Computer wird dich dabei unterstützen.