RaPZ

Sicherheit & Datenschutz

2020

28. JUNI

AGIAMONDO e.V.
Verfasst von: Lukas J. Gorski

AGIAMONDO
Personal und Beratung
für internationale Zusammenarbeit

Inhalt

1 Schutzmaßnahmen 3
1.1 Reele Schutzmaßnahmen 3
1.1.1 Diebstahlsicherung – Kensington-Schloss 3
1.1.2 Lokale IT-Helfer 3
1.1.3 Elektrizität – Überspannung 3
1.1.4 Firewall 4
2 Verschlüsselung 5
2.1 Grundlagen 5
2.2 Containerverschlüsselung 5
2.3 Komplettverschlüsselung 6
2.4 VeraCrypt (Software) 6
3 Backup 6
3.1 Backup Auswahl 7
3.2 Backup Medien 7
3.3 Backup Strategien 7
3.4 Backup Software 8

1 Schutzmaßnahmen

Im ersten Kapitel des Themas Sicherheit und Datenschutz geht es um Schutzmaßnahmen vor ungewolltem Zugriff Dritter auf Daten und Computer sowie durch äußere Einwirkungen. Dies kann physikalische wie auch virtuelle Maßnahmen benötigen.

1.1 Reele Schutzmaßnahmen

VORSICHT!

Lassen Sie, wenn möglich, niemanden an Ihren Computer, dem Sie nicht 100-prozentig vertrauen!

1.1.1 Diebstahlsicherung – Kensington-Schloss

Bei einem Kensington-Schloss in Verbindung mit einem Stahlseil handelt es sich um eine einfache Diebstahlsicherung für mobile Geräte. Auf Seiten des mobilen Gerätes wird das Kensington-Schloss in eine extra dafür vorgesehene Öffnung eingeführt und abgeschlossen. Auf der anderen Seite des Stahlseils befindet sich meist eine Öse, mit der das mobile Gerät an Gegenständen befestigt werden kann.

http://de.wikipedia.org/wiki/Kensington-Schloss

1.1.2 Lokale IT-Helfer

Vorsicht!

Es gibt immer wieder Meldungen darüber, dass lokale IT-Kräfte Trojaner* auf Computern installieren, um diese bewusst auszuspionieren.

* Trojaner sind Programme, die auf dem Computer Informationen sammeln und über das Internet an einen anderen Computer gesendet werden. Alternativ können diese Informationen auch direkt am Computer z.B. auf einen USB-Stick geladen werden.

1.1.3 Elektrizität – Überspannung

In Ländern, in denen nicht die gleichen Standards beim elektrischen Stromnetz wie in Deutschland gelten, müssen Schutzmaßnahmen für elektrisch betriebene Geräte ergriffen werden. Dazu zählt unter anderem ein sogenannter **Überspannungsschutz**. Dieser wird zum Schutz von elektronischen Geräten vor zu hohen Schwankungen der elektrischen Spannungen genutzt. Ein Überspannungsschutz kann in Steckdosenleisten, Sicherungskästen oder in dedizierten Überspannungsschutz-Geräten eingebaut sein.

Empfehlung

- **Ein Überspannungsschutz sollte bereits in Deutschland gekauft werden, da die vor Ort verkauften Geräte teilweise geringe Qualität aufweisen.**
- **Geräte, die nicht benutzt werden, sollten vom Netzstrom physikalisch getrennt werden.**

1.1.4 Firewall

Eine Firewall hilft dabei, die Kommunikation zwischen Netzwerk und Internet zu überwachen, um böswillige Angriffe zu verhindern. Die heutzutage oftmals verwendeten „Router“, die die Einwahl ins Internet automatisch steuern, haben überwiegend alle eine Firewall eingebaut und schützen vor Zugriff vom Internet auf das lokale Netzwerk.

Ab Windows Vista liefert Microsoft sein Betriebssystem mit einer integrierten Windows-Firewall aus. Diese ist in der Lage Programme zu erkennen, die sogenannte „Ports“ öffnen, um Verbindungen von außen anzunehmen. Für die normale Verwendung des Computers, zudem meist noch zusätzlich durch die Firewall im Router geschützt, reicht die Windows-Firewall aus.

Eine Alternative zur integrierten Windows-Firewall ist die Installation eines Firewall-Programmes, welches erweiterte Funktionen bereitstellt. Dazu gehört unter anderem die Benachrichtigung des Anwenders über Programme, die auf das Internet zugreifen möchten. Dies ermöglicht dem Anwender nur bestimmte Programme, denen vertraut wird, Zugriff auf das Internet zu gestatten.

Beachten!

Eine alternative Firewall zu der in Windows integrierten sollte nur dann installiert werden, wenn das nötige Knowhow der Verwendung vorhanden ist. Denn nach der Installation auf dem Computer wird wirklich jede einzelne Verbindung zum Internet überwacht und es muss entschieden werden, welche davon abgelehnt und welche zugelassen werden soll.

Die Comodo Firewall ist eine kostenlose und einfach zu bedienende Firewall. Nach der Installation wird die Netzwerk Kommunikation überwacht und Benachrichtigungen ausgegeben sobald ein Programm Zugriff auf das Internet anfordert. Für bekannte Programme, wie beispielsweise den verwendeten Internet Browser, kann der Zugriff dauerhaft über das Setzen des Hakens „Antwort merken“ gewährt werden.

Beachten!

Bei der Installation wird Zusatzsoftware mitinstalliert, wenn diese nicht abgewählt wird. Nachdem die Installationsdatei gestartet wurde sollten Sie auf „Installation anpassen“

klicken (unten links) und alle Haken, außer die der „Comodo Firewall“ entfernen. Nach dem Klick auf „zurück“ können alle weiteren Haken in der Installation entfernt werden. So wird nur die Firewall installiert.

Downloads:
https://www.comodo.com/home/internet-security/firewall.php
https://tinywall.pados.hu/download.php

2 Verschlüsselung

Sollte der Computer doch einmal unter unerlaubten Zugriff geraten, so bietet die Verschlüsselung von den eigenen Daten eine weitere Sicherheitsbarriere an.

2.1 Grundlagen

Verschlüsselung ist der Vorgang bei dem Informationen, die im Klartext vorliegen, in eine unleserliche Zeichenfolge umgewandelt werden. Ähnlich wie beim Türschloss kann diese regulär nur mit dem richtigen Schlüssel wieder geöffnet werden.

Vorsicht!
Sollten Sie das Passwort zur Entschlüsselung verlieren gibt es keine Möglichkeit mehr Ihre Daten zu entschlüsseln!

Nachfolgend wird das Thema der Festplattenverschlüsselung in den Möglichkeiten der Container- und Komplettverschlüsselung erläutert.

2.2 Containerverschlüsselung

Die Containerverschlüsselung bietet die Möglichkeit bei Bedarf einen gesicherten Ordner zu öffnen, Daten hinzuzufügen, zu bearbeiten oder zu lesen, um diesen anschließend wieder zu verschließen. Diese Form der Datenverschlüsselung bietet zudem die Möglichkeit den verschlüsselten Container auf einem USB-Stick bei sich zu tragen und auf anderen Computern zu öffnen.

Vorsicht!
Es kann passieren, dass nach der Bearbeitung einer Datei aus Ihrem verschlüsselten Container, diese unverschlüsselt im Arbeitsspeicher verbleibt. Dieses Risiko besteht vor allem, wenn Ihr Computer während der Bearbeitung einer solchen Datei abstürzt, in den Standby oder Ruhezustand wechselt.

Hintergrund

Vereinfacht ausgedrückt verschlüsselt die Software den erstellten Container mit einem Passwort, welcher gleichzeitig auch die Entschlüsselung des Containers und das Öffnen des Containers ermöglicht. Beim Öffnen einer Datei aus dem Container wird diese **unverschlüsselt** in den **Arbeitsspeicher** geladen, damit der Computer diese lesen und bearbeiten kann. Bei einem zu kleinen Arbeitsspeicher kann es zudem passieren, dass der Computer Daten aus dem Arbeitsspeicher **temporär** auf die **Festplatte auslagert**.

2.3 Komplettverschlüsselung

Hierbei wird die gesamte Festplatte eines Computers verschlüsselt und bietet bei einem Diebstahl Schutz der gesamten Daten. Dies bietet den besten Schutz, es muss jedoch bei jedem Start des Computers das Passwort zur Entschlüsselung eingegeben werden.

2.4 VeraCrypt (Software)

VeraCrypt (ehemals TrueCrypt) ist eine kostenlose Verschlüsselungs-Software, deren Quellcode offen liegt – Open Source genannt. Die Software ist der Nachfolger von TrueCrypt und basiert auf den gleichen Grundlagen sowie Benutzeroberfläche.

Download: https://veracrypt.codeplex.com/releases

Unter „Recommended Download“ befindet sich stehts die aktuelle Version von VeraCrypt welche für Windows vorgesehen ist. Sollten Sie die Software für Mac OSX oder Linux benötigen so finden Sie einen Download link darunter.
Auf der Website von VeraCrypt gibt es eine Anleitung für die Nutzung des Programmes:

https://veracrypt.codeplex.com/documentation

3 Backup

Unabhängig von böswilligen Angriffen auf Ihren Computer sollen Sie Datenschutzmaßnahmen gegen den Verlust von Daten ergreifen. Dies beugt dem Verlust von Daten durch Festplattendefekte vor wie auch das versehentliche Löschen von Daten.

Hintergrund

Sollte Ihr Computer einmal nicht mehr starten, heißt dies nicht zwangsläufig, dass Ihre Daten verloren sind. Denn ein Computer besteht aus mehreren Einzelteilen, die unabhängig voneinander Defekte aufweisen können. Entscheidend ist der Zustand der Festplatte, dies

können Sie von einem IT-Experten leicht prüfen lassen. Wenn Sie es sich zutrauen können Sie die Festplatte auch selbst in einen anderen Computer einbauen und prüfen ob der Test-Computer damit startet.

3.1 Backup Auswahl

Die Frage welche Dateien gesichert werden sollen, richtet sich auch immer an den Anwender selbst. Grundsätzlich sollten alle Dateien, die nicht verloren gehen dürfen, gesichert werden. Dazu bietet es sich an, einen Ordner in den eigenen Dateien anzulegen und in diesem Unterordner für die jeweiligen Dokumente und Dateien anzulegen. So liegen alle wichtigen Dateien an einem Ort und können leicht gesichert werden.

Neben dem Sichern von selbst erstellten Dateien wie Word- oder Excel-Dokumente, spielen bei der Sicherung auch Daten und Dateien, die von Programmen erstellt wurden eine Rolle. Als Beispiel kann hier Microsoft Outlook genannt werden. Das Email Programm speichert die empfangenen Emails in einer speziellen Datei, welche auch gesichert werden kann. Jedes Programm speichert die Anwendungsdaten an unterschiedlichen Orten, wodurch eine programmspezifische Recherche für jedes Programm vor dem Backup durchgeführt werden sollte.

3.2 Backup Medien

Als Backup Medien können USB-Sticks oder externe Festplatten verwendet werden, wie auch CDs oder DVDs die meist nur einmal beschrieben werden können.

Bei kleinen Sicherungsdatenvolumen von bis zu einem Gigabyte spielt vor allem die persönliche Präferenz bei der Auswahl eine Rolle. Geht es um die Sicherung von täglichen größeren Datenmengen sollten Sie sich genauer mit dem Thema Backup befassen und gegebenenfalls weiteren Rat einholen.

3.3 Backup Strategien

Bei der Sicherung von Daten wird zwischen verschiedenen Möglichkeiten der Sicherung unterschieden. Am meisten verbreitet sind die Voll-Sicherung, bei die ausgewählten Dateien vollständig gesichert werden und die Inkrementelle-Sicherung, bei der nur die Dateien aus der Auswahl gesichert werden, die sich seit der letzten Voll-Sicherung geändert haben.

Sicherungsdatenvolumen von bis zu einem Gigabyte sollten einfach gehalten werden. Hier ist die Empfehlung eine tägliche Voll-Sicherung mit einer Woche Vorhaltezeit des Backups. Dadurch besteht der Zugriff auf die letzten 7 Tage und sollte einmal ein Backup fehlerhaft sein, wirkt sich dies nicht auf die anderen Backups aus.

Bei größeren Datenmengen bietet sich aus Platz- und Performancegründen eine erweiterte Strategie an. Für die Sicherung von großen Datenmengen, die vor allem in der Woche bearbeitet werden, ist die Voll-Sicherung der Daten am Ende der Woche, meist Freitagabends und darauf aufbauend eine Inkrementelle-Sicherung in der Woche, Montag bis Donnerstag optimal. Dadurch werden die Vorteile beider Sicherungsverfahren ausgenutzt.

3.4 Backup Software

In Windows 7, und allen folgenden Windows Versionen, ist eine Backup Software bereits enthalten. Diese ist über die Systemsteuerung zu erreichen und trägt den Namen „Sichern und Wiederherstellen“. Mit Hilfe dieses Tools können automatische Backups von Dateien auf externe Festplatten, DVDs oder CDs gesichert werden. Um dieses zu konfigurieren müssen die folgenden Schritte durchgeführt werden:

- Öffnen Sie über das **Startmenu** die **Systemsteuerung**, klicken Sie auf **System und Sicherheit**, darauffolgend auf Sichern und Wiederherstellen
- Für die Einrichtung des ersten Backups klicken Sie auf **Sicherung einrichten** und folgen den Anweisungen
- In dem darauffolgenden Menu kann gewählt werden zwischen der **Auswahl durch Windows** oder **Auswahl durch Benutzer** für die zusichernden Dateien.

Empfehlung

Wählen Sie die **Auswahl durch den Benutzer** und Erstellen Sie dafür einen neuen Ordner in Ihren Eigenen Dateien. In diesen werden alle alle wichtigen Daten herein kopiert. Dieser Ordner kann nun als zusichernder Ordner ausgewählt werden.