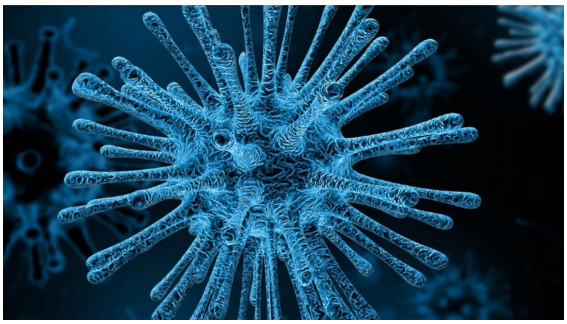
IT-Sicherheitstipp Nr.7 – September 2019

Gefahren durch Viren

Was ist eigentlich ein Computervirus?



Viren (auch „Schadprogramm“, „Malware“ etc. genannt) sind kleine Computer-Programme oder Programmteile, die unerwünschte Aktionen auslösen und verschiedenste Auswirkungen auf Ihr Computersystem haben können:

- In der harmlosesten Stufe sind Viren nur lästig oder stiften Verwirrung, z. B. durch ungewöhnliche Aktionen, die Ihre Daten aber nicht beschädigen.
- Andere Viren nutzen Ihr System, in dem sie Programme missbrauchen, z.B. Ihr E-Mail-Programm verwenden, um E-Mails an alle Adressen in Ihrem Adressbuch zu senden oder diese abzugreifen.
- Manche Viren spionieren Passwörter aus, verändern Dateien oder zerstören im schlimmsten Fall ganze Systeme.
- Seit einiger Zeit gibt es verbreitetet Viren, die Ihre und die Daten Ihrer Verwaltung verschlüsseln. Der Schlüssel zum Entschlüsseln wird im Anschluss zum Kauf angeboten (sog. Ransom-Ware; Ransom = Erpressung).

Die Bandbreite ist also groß. Täglich werden ca. tausend neue Viren in Umlauf gebracht. Längst liegen die durch Viren verursachten Schäden in Millionenhöhe.

Hohe Artenvielfalt
Viren-Typen

Häufig wird der englische Oberbegriff „Malware“ („mal“ = engl. für „schädigend“) für alle Virenarten verwendet. Man unterscheidet zwischen unterschiedliche Typen von Malware bzw. Viren:

Datei-Viren:
Datei-Viren stellen die klassische Form eines Computervirus dar. Sie befallen bestimmte Dateien, wie etwa ausführbare Programme und vermehren sich beim Aufruf dieser Programmdateien.

Trojanische Pferde:
Sogenannte "Trojaner" werden genutzt, um weitere Schadprogramme wie etwa Bots auf Ihren Computer zu schleusen, um z.B. Daten und Passwörter auszuspionieren, das System unbemerkt für Zugriffe von außen zu öffnen, Ihren Rechner für Angriffe auf andere Systeme zu verwenden oder Ihre Daten zu verschlüsseln und Sie dann zu erpressen.

Würmer:
Die Virenart „Wurm“ ist ein selbstständiges, selbstreproduzierendes Programm, das sich bevorzugt in Netzwerken ausbreitet und versucht, dessen Arbeit zu stören. Ihr Gefährdungspotenzial ist vergleichbar mit dem von Dateiviren und Trojanischen Pferden.

Bots:
Bots (als Abkürzung für „robots“) sind selbstständig arbeitende Computerprogramme, die ohne Zutun des Nutzers aktiv sind. Problematisch ist dies, wenn sie im Verborgenen agieren. Ein im PC „versteckter“ Bot wird Angriffe auf Webseiten durchführen oder Daten Ihres Computers „stehlen“.

Hoax:
Ein Hoax ist kein Virus sondern eine Art „schlechter Scherz“, oft im Kettenbriefformat. Ein Beispiel für einen Kettenbrief sehen Sie links oben. Erst durch die Weiterleitung an andere wird die beabsichtigte Wirkung eines „Virus“ entfaltet, nämlich die „automatische“ massenhafte Verbreitung. Kettenbriefe findet man heute vornehmlich in sozialen Netzwerken.

Cybersicherheit

Mögliche Schäden durch Virenbefall

Je nach Virus sehen die verursachten Schäden sehr unterschiedlich aus. Früher war das Hauptangriffsziel die Störung der Systemfunktionen z.B. durch:

- Verbrauch von Systemressourcen wie Plattenplatz oder Leitungskapazitäten
- Verringerung der Systemleistung
- Verändern oder Löschen von Systemdateien

Ziel von Viren sind meistens unerwünschte Aktionen, wie z.B. das heimliche Versenden von Spam-E-Mails. Häufig geht es aber auch um das **Ausspionieren von Daten** oder die Verwendung des Rechners als Plattform für Angriffe auf andere Systeme (sog. Denial of Service-Angriffe).

Gefährlich werden Viren, wenn sie sich unbemerkt einschleichen und z.B. wochen- oder monatelang unbemerkt das System und Behördennetz nach internen Informationen ausspionieren. Davon sind auch vermeintlich unwichtige Arbeitsplätze z.B. in der Sachbearbeitung als „Einfallstor" betroffen.

Einige Trojaner behaupten durch ein großes Bild, dass Ihr Computer für illegale Zwecke eingesetzt worden sei. Das Bundeskriminalamt habe ihn gesperrt und könne ihn gegen eine „Bußgeldzahlung" wieder freigeben. Manche Trojaner verschlüsseln Ihre Festplatte und fordern „Lösegeld". Hier hilft oft nur den Computer völlig neu einzurichten. Wieder andere Programme missbrauchen Ihren Computer, um ungefragt dessen Rechenleistung zu nutzen.

Heutzutage wird häufig über „Bot-Netze" und „gekaperte" Rechner oder „Zombies" gesprochen.

Hier ist eine kurze Erklärung, wie das funktioniert:

1. Ein erster Angreifer streut breit einen Virus und infiziert mehrere Computer.
2. Die infizierten („gekaperten") Computer („Zombies") melden sich (unbemerkt vom Benutzer) an einem Server an und bilden zusammen ein Netzwerk („Bot-Netz").
3. Ein zweiter Angreifer (z.B. Spammer) mietet beim ersten einen Zugang zur Bot-Netz-Steuerung.
4. Der zweite Angreifer erteilt dem Bot-Netz eine Aufgabe (z.B. „Versendet Werbung für XXX!").
5. Der gekaperte Computer führt zusammen mit den anderen Zombies verdeckt die Aufgabe aus und wartet auf weitere Befehle.

Infektionswege
Viren erreichen auf verschiedenen Wegen ihr Ziel:

- Der Hauptinfektionsweg ist die E-Mail. Unter Umständen kann schon durch das bloße Lesen einer E-Mail ein Virus aktiv werden (etwa wenn die Auto-Vorschau aktiv ist). Besonders gefährlich ist es, mitgeschickte Dateien zu öffnen.
- Auch durch das Starten von Dateien, die Sie aus dem Internet herunterladen, kann ein Virus aktiv werden. Manchmal reicht sogar das Aufrufen einer infizierten Web-Seite.
- Auch das interne Behördennetz kann Ausgangspunkt von Viren sein. Sie können in abgespeicherten Dokumenten oder Programmteilen vorliegen und sich über verbundene Netzlaufwerke automatisch verbreiten oder selbst versenden.
- Externe Speichermedien wie USB-Sticks können Viren enthalten - selbst Originale vom Hersteller oder auch der USB-Stick aus der hilfsbereiten Kollegenschaft sind möglicherweise infiziert. Auch Smartphones und Digitalkameras, die mit dem Behördennetz verbunden werden, können Viren übertragen.
- Ein nicht zu unterschätzendes Risiko besteht beim Datenaustausch per Smartphone, USB-Stick oder transportabler Festplatte zwischen heimischem PC und Computer im Büro.

**Manche Verwaltungen verschließen deshalb USB-Buchsen am Computer mechanisch oder per Software.
Respektieren Sie dies zum Schutz der Verwaltung sowie Ihrer Geräte!**

LANDKREIS MARBURG BIEDENKOPF

Projekt der interkommunalen Zusammenarbeit

Cybersicherheit

Landkreis Gießen
HESSENS MITTE • WISSEN WIRTSCHAFT & KULTUR

Risiken und Schäden
Risiken steigen mit dem Anschluss ans Internet.

Wann immer Daten von außen auf einen Rechner übertragen werden, besteht das Risiko eines Virenbefalls. Mit der steigenden Nutzung des Rechners als Kommunikationsmedium steigt auch die Virengefahr. Sobald ein Internetanschluss vorliegt, liegt die Wahrscheinlichkeit eines Virenangriffs bei 100 %.

Das heißt: Ohne Virenscanner ist eine Infektion praktisch unvermeidlich!

Der drohende Schaden kann beträchtlich sein:

Werden durch einen Virenbefall Daten zerstört, so entstehen Ihrer Verwaltung gegebenenfalls hohe Aufwände bei der Wiederherstellung. Gelangen ausspionierte Daten an die Öffentlichkeit, so können Ihrer Organisation Ansehens- und Vertrauensschäden entstehen, von Datenschutzverstößen ganz zu schweigen.

Selbst wenn keine Informationen gelöscht oder ausspioniert werden, kann das Wiederherstellen befallener Systeme zeitaufwändig sein und hohe Kosten verursachen.

Vorbeugemaßnahmen gegen Virenbefall
Wie in der Medizin gilt: „Vorbeugen ist besser als Heilen“.

- Um befallene Dateien von Viren zu säubern, gibt es speziell dafür geschriebene Programme, sogenannte Virenscanner.
- In den meisten Verwaltungen werden alle Server und PCs mit einem Virenscanner ausgestattet, der eingehende E-Mails untersucht.
- Auch jeder Privat-PC sollte immer durch einen aktuellen Virenscanner geschützt sein.
- Das Virenscanner-Programm untersucht alle Daten auf Ihrem Computer vor dem Zugriff oder Speichern auf Viren. Es darf deshalb nie ausgeschaltet werden.
- Der Virenscanner muss so eingestellt sein, dass immer alle Daten in Echtzeit auf Viren überprüft werden („On Access“).
- Für mobile Endgeräte gibt es ebenfalls Viren und Virenscanner-Anwendungen („Apps“).

- Der Virenscanner selbst muss so eingestellt sein, dass er sich mindestens täglich selbstständig aktualisiert. Sollte wider Erwarten eine Meldung erscheinen, dass der Scanner veraltet ist, informieren Sie bitte direkt ihre IT-Abteilung.
- Zusätzlich sollte der Virenscanner so eingestellt werden, dass er einmal pro Woche das gesamte System automatisch auf Viren überprüft („On Demand“).
- Auch ein aktueller Virenscanner bietet keinen 100%igen Schutz. Deshalb sollten Sie, wenn möglich, Ihre Daten auf Netzlaufwerken speichern. Sie werden in den meisten Behörden von dort regelmäßig gesichert und können nach einem Schaden wieder hergestellt werden.

Virenbefall – Was tun?
Don't panic – Ruhe bewahren

Wenn Sie vermuten, dass sich ein Virus eingeschlichen hat, ist eine schnelle Reaktion gefragt, um größeren Schaden zu vermeiden.

Wichtig ist dabei:

- Geraten Sie nicht in Panik!
- Computer vom Netzwerk trennen, also Kabel ziehen oder drahtlose Verbindung abschalten
- Auf keinen Fall eigene Bereinigungsaktionen durchführen
- Benachrichtigen Sie Ihre IT-Abteilung. Sie kümmert sich um die weiteren Schritte zur Beseitigung des Virus und zur Wiederherstellung betroffener Daten.
- Wenn Sie Zugriff darauf haben, halten Sie die letzte Datensicherung bereit.
- Wenn der Virus Sie zur Zahlung eines „Lösegelds“ auffordert, informieren Sie ebenfalls Ihre Ansprechperson.

Leisten Sie keinesfalls selbst Zahlungen! Im Zweifelsfall ist beides weg – Daten und Geld

Bei Fragen wenden Sie sich bitte an Ihre Informationssicherheitsbeauftragten oder die Projektleitung Cybersicherheit.

Eine gemeinsame Sensibilisierungskampagne zur Informationssicherheit der Landkreise Marburg-Biedenkopf

und Gießen im Rahmen des IKZ-Projekts Cybersicherheit.

Geht mich nichts an?
Mit Sicherheit!