KOM SG

Merkblatt Verhalten bei Verdacht auf Malwarebefall

Am besten ausdrucken und griffbereit deponieren

Was versteht man unter Malware?

Malware ist der Oberbegriff für verschiedenartige Schadsoftware, die einer bösartigen Absicht dienen. Da es sehr viel unterschiedliche Malware-Arten gibt, sind auch die Symptome sehr unterschiedlich.

Mögliche Symptome bei Befall mit Malware

Bitte beachten Sie, dass die meisten Fehler vereinzelt auch ohne Malware auftreten können. Wenn diese Symptome aber z.B. nach dem Anschliessen eines USB Stick, dem irrtümlichen Öffnen einer merkwürdigen Mail oder einer intensiveren Internet-Recherche auftreten, ist die Gefahr gross, dass es sich um eine tatsächliche Malware handelt. Hier gilt: Besser ein Alarm zu viel, als einer zu wenig!

- Die Antiviren-Software oder der Windows Defender melden, sie hätten einen Virus gefunden.
- Das System stürzt ab, der Rechner fährt unerwartet herunter oder lässt sich nicht mehr starten.
- Bestimmte Funktionen lassen sich nicht mehr ausführen.
- Programme arbeiten fehlerhaft oder stürzen ab.
- Plötzlich sind neue unbekannte Programme installiert, poppen auf oder führen Funktionen aus.
- Der Mauszeiger bewegt sich ohne Ihr Zutun.
- E-Mails werden automatisiert unter Ihrem Namen verschickt.
- Dann die eindeutige Ansage: Am Bildschirm erscheint die Meldung einer Erpressersoftware (Ransomware), dass die Dokumente verschlüsselt worden seien.

Die nächsten beiden Punkte sind zwar auch typisch bei einem Malwarebefall, haben aber meist andere Ursachen und sind deshalb schwerer zuzuordnen.

- Der Rechner arbeitet im gewohnten Betrieb deutlich langsamer als sonst. Die mögliche Ursache ist dabei allenfalls eine erhöhte Prozessorauslastung durch Malware.
- Das Internet ist wesentlich langsamer als sonst, aufgrund eines erhöhten Datentransfers durch die Malware.

Was tue ich im Fall der Fälle?

- Trennen Sie Ihren Rechner **sofort** vom Netz:
  - Entfernen Sie das Netz-Kabel und schalten Sie Ihr WLAN aus.
  - Bei einem PC: Ziehen Sie einfach das Stromkabel raus, dann schaltet sich der Rechner sofort ganz ab.
  - Zur Not drücken Sie am Notebook solange den Einschaltknopf, bis sich das Gerät auf einen Schlag ausschaltet und nicht nur in den Ruhemodus geht.
- Informieren Sie sofort Ihre informatikverantwortliche Person (IV).

- Beschreiben Sie Ihrem IV möglichst genau, was passiert ist, damit er über das weitere Vorgehen entscheiden kann.

- Eröffnen Sie unbedingt gleichzeitig ein Ticket bei Abraxas. Dies kann auch ein Kollege in Ihrem Namen tun. Alternativ können Sie die **Abraxas Hotline** auch über Ihr eigenes Telefon anrufen.
  Tipp: hinterlegen Sie die Nummer in Ihrem Adressbuch: **+41 58 660 0011**
- Sollten Sie zuvor einen USB Datenträger angeschlossen haben oder war kurz vorher einer angeschlossen, erwähnen Sie das bitte bei Ihren Meldungen an IV und Abraxas und halten Sie den Datenträger bereit. Vernichten Sie ihn also nicht und geben ihn auch nicht weiter.
- Schalten Sie den Computer nicht wieder ein und stellen Sie ohne Aufforderung ihres IV oder von Abraxas insbesondere keine Netzwerkverbindung her.
- Greifen Sie auf verdächtige Mails und Links nicht mit einem zweiten Client oder einem Smartphone zu. Tun Sie dies auch nicht über Ihr WebMail.