Achtung: Erpressungs-Trojaner!

Die Verbreitung von Schadsoftware, insbesondere von sogenannten Erpressungstrojanern (Ransomware), hat in den letzten Monaten weltweit massiv zugenommen.

Die Schadsoftware gelangt z.B. durch manipulierte Office-Dateien (Schadcode in Makros) als E-Mail-Anhänge auf die betroffenen Rechner. Daneben kann die Schadsoftware auch durch sogenannte Drive-by-Downloads auf den Rechner gelangen. Dies geschieht durch surfen auf infizierten Webseiten, hervorgerufen durch Sicherheitslücken im Browser. Im Falle der aktuellen Erpressungstrojaner werden komplette Festplatten und Netzwerklaufwerke verschlüsselt und unbrauchbar gemacht. **Aktuelle Virenscanner allein helfen hier nicht!**

Folgende Tipps schützen Sie vor Bedrohungen aus dem Internet:

• Dateien und Dateianhänge (E-Mail, USB-Stick, Internet, etc.):
Öffnen Sie keine Anhänge, an deren Vertrauenswürdigkeit auch nur der geringste Zweifel besteht. Oft werden Nachrichten mit üblichen Betreffzeilen, wie z.B. "Rechnung" o.ä. getarnt. **Diese E-Mails können auch von vertrauenswürdigen und Ihnen bekannten Personen kommen.**

• Ausführbare Dateien / Software:
Starten Sie auch keine ausführbaren Dateien, (.exe, .bat, .com, etc.) sofern diese nicht aus einer vertrauenswürdigen Quelle stammen bzw. der Ursprung nicht bekannt ist.

• Gefälschte E-Mail-Nachrichten:
Achten Sie auf Nachrichten mit einem Betreff wie: „Verifizieren Sie Ihren Bankzugang, Ihr amazon- oder PayPal-Konto oder Ihren eBay-Account.“ Hinter den meisten Nachrichten dieser Art stehen sog. Phishing-Attacken, die Zugangsdaten wie Passwörter und PIN-Nummern abgreifen wollen.

• Deaktivieren Sie Makros:
Deaktivieren Sie Makros oder konfigurieren Sie Microsoft Office so, dass der sogenannte Makro-Code nicht oder erst nach einer Rückfrage ausgeführt werden kann.

• Internetsurfen – aber sicher:
Surfen Sie nur auf Internetseiten, deren Vertrauenswürdigkeit möglichst gesichert ist. Achten Sie darauf, bei der täglichen Arbeit nicht mit Administrationsrechten zu surfen. Definieren Sie ein eigenes Benutzerkonto mit eingeschränktem Zugriff und arbeiten Sie darüber.

• Backups:
Backups schützen vor Datenverlust. Wir empfehlen daher Backups in regelmäßigen Abständen durchzuführen. Des Weiteren sollten die Backup-Medien vom Rechner getrennt werden. Sonst könnten auch diese verschlüsselt werden.

• System-Updates:
Halten Sie Ihr System (Betriebssystem, Microsoft Office, Browser, Java, Flash) immer auf dem aktuellen Stand. **Bei unbekannten Update-Dialogen ist Achtung geboten! Gehen Sie hier mit der gleichen Vorsicht vor, wie beim Öffnen unbekannter Dateien.** Bei Updates generell ist darauf zu achten, dass keine unbekannten Erweiterungen (Toolbars, Tools, etc.) mitinstalliert werden.

• Virenscanner:
Virenscanner bieten einen umfassenden Virenschutz. Installieren Sie daher einen Virenscanner und laden Sie regelmäßig Updates herunter. Die parallele Verwendung mehrerer Virenscanner bietet keinen Mehrfachschutz.

Fazit:
Ein 100%iger Schutz ist leider nicht möglich. Durch ein entsprechendes Verhalten kann das Risiko aber deutlich minimiert werden. Weitere Informationen finden Sie unter www.bsi.bund.de.