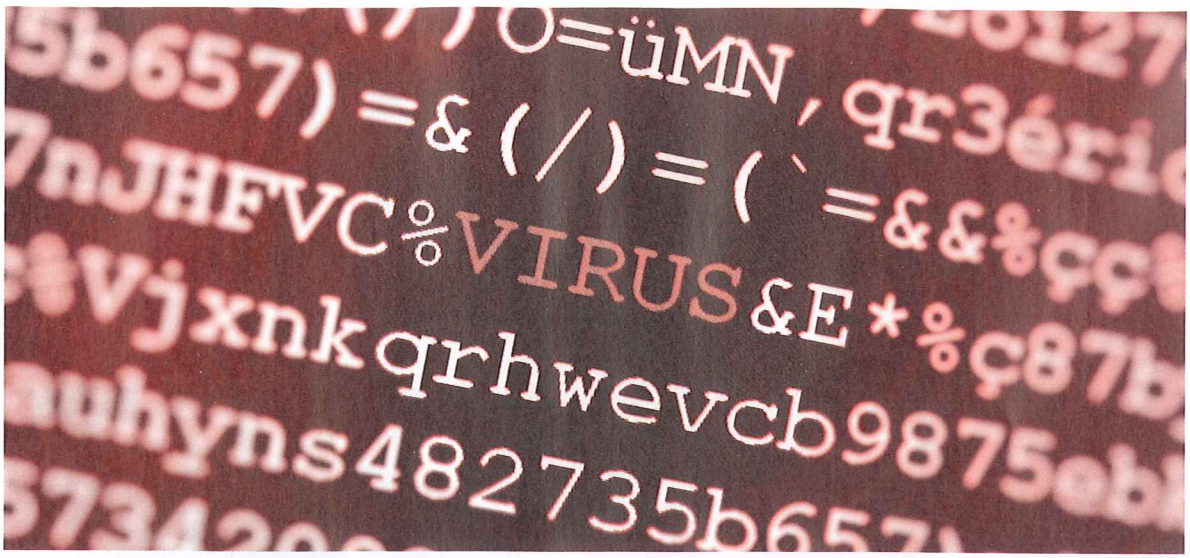

Ein echter Albtraum: Virus versperrt den Zugang zu Dateien

Computerviren verschlüsseln aktuell auch in Bayerisch-Schwaben Unternehmensdaten auf Rechnern und in Netzwerken. Sicherheitsmaßnahmen und regelmäßige Datensicherungen minimieren das Risiko und sorgen dafür, dass im Schadensfall der Betrieb weiterlaufen kann.

So hart es für diejenigen ist, die von Locky oder anderen Cryptolockern heimgesucht werden: Sie erfahren sofort, dass sie ungebetene Gäste hatten. Die Folgen sind sofort spürbar, alle Daten auf den lokalen Rechnern und oft auch im zugänglichen Netzwerk sind verschlüsselt, ein Zugriff ist nicht mehr möglich. Um den Betrieb aufrechtzuerhalten, bleibt nur noch, die betroffenen PCs durch Experten säubern zu lassen und die letzte Datensicherung aufzuspielen. Glück für den, der zumindest an dieser Stelle auf IT-Sicherheit gesetzt hat.

Doch leider gibt es auch unzählige Angriffsmuster, die keine sichtbaren Spuren hinterlassen und im Verborgenen agieren. Zugang verschaffen sich Cyberkriminelle oft durch Softwareschwachstellen (Exploits) oder unzureichende Sicherheitseinstellungen, die es erlauben, Schadcodes auf einem PC auszuführen. Durch E-Mails mit schadhaften Dateianhängen oder manipulierte Websites gelangen die Hacker in Netzwerke. Dort agieren sie im Hintergrund, bis zur vollständigen Übernahme des Rechners oder des gesamten Netzwerks.

Um Schäden abzuwenden, brauchen Unternehmen ein funktionierendes Sicherheitskonzept, das mindestens folgende Punkte umfassen sollte:

- Sensibilisierung aller Nutzer für IT-Sicherheit
- Vorsicht bei allen E-Mails
- regelmäßige Updates aktiver Software
- Einsatz leistungsfähiger Virenschutz- und Firewall-Technologie
- sinnvolle und sorgsame Rechtestrukturen
- regelmäßige Sicherung aller geschäftsrelevanten Daten
- Notfallplan zur Wiederherstellung der Systeme

Ist der „Sandkasten" die neue Wunderwaffe?

Ein Ansatz, um sich künftig besser vor Angriffen schützen zu können, ist der Einsatz von Sandboxing-Technik. Dabei werden Dateianhänge und Downloads zunächst in einer gekapselten Box (Sandbox) ausgeführt und auf Verhaltensauffälligkeiten geprüft. Werden Auffälligkeiten festgestellt, wird dem Benutzer der Zugriff verwehrt und der Administrator informiert.

Mehr IT-Sicherheit erfordert manchmal Einschränkungen beim Benutzerkomfort. Aber im Auto würde auch niemand aus Bequemlichkeit auf den Sicherheitsgurt verzichten.

Armin J. Schweikert, Parit GmbH, Augsburg

Ansprechpartner:
DR. KRISTIN JOEL
Fachbereich Technologie und IT
Tel.: 0821 3162-406
kristin.joel@schwaben.ihk.de

IT-Sicherheit in Schwaben: IHK kooperiert mit aitiRaum e. V.

Die IHK Schwaben bietet in Kooperation mit dem Netzwerk aitiRaum e. V. Veranstaltungen und Informationsmaterial zum Thema „IT-Sicherheit für Familienunternehmen".
Den vollständigen Warnhinweis sowie weitere Informationen und Links zur IT-Sicherheit finden Sie unter www.schwaben.de, Nr. 2706258