

PRÄVENTIVE MASSNAHMEN GEGEN RANSOMWARE

So schützen Sie sich vor der Erpressungs-Malware und vermeiden kostenintensive Betriebsausfälle

Durch genügend Vorsicht können Sie Cyber-Angriffe weitgehend vermeiden. Folgende technische und organisatorische Maßnahmen bieten Ihnen einen soliden Schutz vor den Angriffen aus dem Netz.

- Reduzieren Sie Infektionsgefahren durch geeignete Firewall-Lösungen sowie durch ausgeklügelte E-Mail- und Web-Security-Konzepte.
- Führen Sie für sämtliche externe Geräte Kontrollen durch. Nur ausgewählte Massenspeicher sollten für den täglichen Gebrauch zugelassen werden.
- Sensibilisieren Sie die User für mögliche Gefahren. Ihr Ziel sollte es sein, aufmerksame Anwender zu formen, die E-Mails hinterfragen und eine bewusste Web-Nutzung an den Tag legen.
- Installieren Sie sinnvolle Anti Virus-Scanner auf allen Endgeräten.
- Halten Sie Ihre Systeme aktuell. Nutzen Sie dafür ein Patch-Management-System, das die Sicherheit auf Clients und Servern automatisch erhöht.
- Unterbinden Sie durch moderne Firewall-Systeme den Datenaustausch mit den Systemen der Angreifer (zum Beispiel durch das Nachladen von Schadcode).
- Suchen Sie sich Unterstützung bei einem kompetenten Partner.

Eine hundertprozentige Sicherheit gibt es leider nicht. Sollte es also, trotz ausreichenden Sicherheitsvorkehrungen, zu einer Infektion kommen, müssen Sie den Schaden so gering wie möglich halten. Folgende Maßnahmen helfen Ihnen, den Sicherheitsvorfall schnell zu beheben und hohe Ausfallkosten zu sparen.

- Richten Sie Berechtigungskonzepte ein. Überlegen Sie dabei, welche Zugriffe/Rechte der User wirklich benötigt.
- Führen Sie ein intelligentes Backupkonzept, das die schnelle Wiederherstellung Ihrer Daten ermöglicht.
- Erstellen Sie einen Notfallplan für Sicherheitsvorfälle. Legen Sie genau fest, welche Maßnahmen im Angriffsfall, nach welcher Reihenfolge, eingeleitet werden müssen.
- Konfigurieren Sie ein ausführliches und intelligentes Logging, um Angriffe frühzeitig zu erkennen und schnell Schwachstellen aufzudecken.
- Etablieren Sie das Thema Security als Prozess, in dem eine regelmäßige Hinterfragung stattfinden soll.

