Handlungsempfehlung bei aktueller Bedrohung

stepIT.net

Aktuell bedrohen weltweit Verschlüsselungstrojaner die Datensicherheit von Firmen. Egal welcher Name, das Ergebnis ähnelt sich für die Betroffenen. Wichtige lokale und im Netzwerk erreichbare Dateien werden individuell verschlüsselt und nur durch eine Zahlung in einer anonymisierten Währung wieder zugänglich. Die kriminellen Hintermänner verdienen so viel Geld mit den Erpressungsversuchen, dass es sich für sie lohnt, die Erstellung eines individuellen Schädlings nach dem Baukastenprinzip, gegen eine Umsatzbeteiligung anzubieten.

Die veröffentlichten Neuinfektionszahlen legen nah, dass die etablierten Schutzmechanismen vor dieser Art der Bedrohung keinen ausreichenden Schutz bieten. Auch Kunden, die sich an dem generellen Sicherheitsstandard halten, sind nicht sicher!

Die IT Landschaft muss sich auch aus diesem Grund anpassen. Wir erstellen mit Ihnen eine IST-Analyse Ihrer IT Systemlandschaft mit Fokus auf die aktuelle Bedrohungslage durch Verschlüsselungstrojaner und anderem Schadcode. Aus der Analyse geht eine Risikobewertung hervor mit einer klaren Handlungsempfehlung für ihr Unternehmen.

Damit Sie sich selbst orientieren können überprüfen Sie ihre Umgebung auf folgende Standards. In eine Verfahrensempfehlung fließt oftmals eine Kombination der folgenden Punkte unter Berücksichtigung und Tuning von Bestandskomponenten und Software ein. Sprechen Sie uns an!

Netzwerk
Das granulare Aufteilen voneinander durch Firewall-Regeln geschützten IP Netzen in z.B. Servernetzwerk, Managementnetzwerk, Client mit E/A Verhalten, Client ohne E/A Verhalten und
Produktionsmaschinen stellt die Grundlage für das Absichern auf Netzwerkbasis dar. Die verschiedenen IP Netzwerke werden durch VLANs sicher voneinander getrennt. Der Traffic zwischen den Netzwerken wird durch Firewall-Regeln reglementiert und unter Zuhilfenahme moderne Sicherheitsstandards überprüft.

Firewall
Server- und Clientsoftware kommunizieren über definierte Kommunikationskanäle. Wer diese durch restriktive Firewall-Regeln kontrolliert, bietet Schadsoftware wenig Möglichkeiten, Einsatzbefehle aus dem Internet abzurufen oder interne Informationen nach außen zu senden.

Virenschutz
Ein flächendeckender Virenschutz muss in jedem Unternehmen vorhanden sein. Nur so kann bekannter Schadcode erkannt und bereinigt werden.

Antispam
Das unnötige Lesen unerwünschter E-Mails vergeudet nicht nur wertvolle Arbeitszeit und Speicher. Durch eine optimierte Antispam Lösung wird schon ein Großteil der mit Schadcode behafteten E-Mails an der Eingangstür des Unternehmens abgewiesen.

Makrosicherheit
Das Ausführen von Programmcode in Office Dokumenten muss für alle Mitarbeiter verhindert werden und nur in definierten Fällen erlaubt sein.

Proxy Server
Klassische Viren und anderer Schadcode verbreiten sich meist über vermeintlich harmlos wirkende Webseiten. Ob diese nun für diesen Zweck erstellt oder eine etablierte Seite unbemerkt "gehackt" wurde, spielt für den Betroffenen keine Rolle. Nur das konsequente Überprüfen dieser Art der Kommunikation bietet einen Schutz!

Rechtemanagement
Nur Informationen die ein Benutzer lesen kann, können unbemerkt an einen Dritten gelangen. Dateien können nur verschlüsselt werden, wenn der Benutzer einen Schreibzugriff auf diese hat. Ein restriktiver Umgang mit Benutzerrechten auf den Datei-Servern wendet viel Schaden ab.

Datensicherung
Bei einem Datenverlust ist nicht selten die Datensicherung die einzige Möglichkeit wieder an die Daten zu gelangen. Eine tägliche Sicherung ist aufgrund der Schnelllebigkeit der Firmendaten keine Alternative mehr. Heute muss eine Datensicherung Systeme mit Umlaufdaten mehrmals untertägig sichern können, um im Wiederherstellungsfall den Datenverlust und die damit verbundene Nacharbeit so klein wie möglich zu halten.