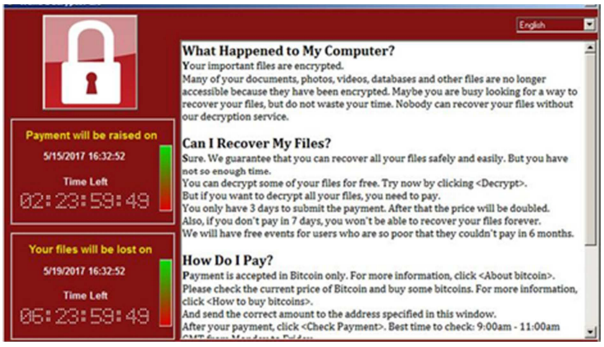
Wir haben eine Lösung gegen Ransomware!



Schwachstelle Mensch: Was tun?

Wer denkt, er sei vor Ransomware sicher, da Firewalls und Virenscanner immer Up-To-Date sind, der irrt. Wie die Angriffe der vergangenen Zeit gezeigt haben stellen diese Systeme keinen Schutz vor den neuesten, modifizierten Schädlingen dar. Die Angriffe werden immer ausgefeilter und zielen ganz klar auf die größte Schwachstelle ab: den Endanwender.

Backups anlegen, Updates und Patches installieren, unsichere Webseiten vermeiden, nur Emails sowie Email-Anhänge von bekannten Absendern öffnen, etc. sind Dinge die in einer professionellen Unternehmens IT schon seit Jahren Standard sein sollten – und dennoch führen Angriffe immer und immer wieder zum Erfolg. Und warum? Weil Ransomware immer raffinierter wird und nicht jeder Endanwender immer aufmerksam ist.

Somit kann man nur noch da ansetzen wo man eine Infektion zuerst entdeckt: Auf dem betroffenen Endgerät oder eben auf dem Netzwerk.

In den letzten Jahren haben sich gerade in großen Unternehmen die NAC (Network Access Control) Systeme durchgesetzt, um die Sicherheit im Netz weiter zu erhöhen. Diese Systeme lassen sich mit Real Time Traffic Scannern zu einem nahezu perfekten Schutzschild gegen Ransomware Angriffe ausbauen.

Durch die Kopplung des NAC Systems mit einem Realtime Traffic Scanner lassen sich Ransomware Angriffe erfolgreich abwehren. Wichtig dabei ist, dass nicht nur bekannte sondern auch noch unbekannte Schadsoftware in Echtzeit erkannt und abgewehrt werden kann.

Zum Erkennen der Ransomware Aktivitäten wird im Netzwerk der Traffic beobachtet und in Echtzeit ausgewertet. Ist ein Schädling aktiv steigt die Zahl der Schreib/Lese Vorgänge sprunghaft an.

Auch die Signatur von Ramsomware kann bei schon bekannten Schädlingen in den Netzwerkpaketen ermittelt werden.

Die IT Abteilung hat die komplette Entscheidung bei der Implementierung wie beim Erkennen von potenziellen Infektionen verfahren werden soll.

So kann das System „nur“ Alarmieren, die betroffenen Endsysteme in ein Quarantänenetz verschieben oder eben die infizierten Endgeräte hart vom Netzwerk abhängen, um eine weitere Verbreitung der Ransomware im Netzwerk zu verhindern.

Somit ist eine Infizierung zwar nicht mehr ausgeschlossen, aber die Verbreitung einer Infektion über unzählige Server und Endgeräte hinweg kann in nahezu Echtzeit gestoppt werden.

Diese zeitnahe Weitergabe der Information an die IT ist von immenser Wichtigkeit, um sofort die richtigen Maßnahmen treffen zu können.