Ransomware Beschreibung – was ist das?

Was ist Crypto-Ransomware eigentlich?

Zitat aus einem Beitrag über Ransomware von Emsisoft: Link

> *Ransomware ist eine Malware, also bösartige Software, die auf Ihrem Computer gespeicherte Dateien, Geschäftsdaten und persönliche Erinnerungen „kapert“. Es gibt zwei wesentliche Typen: Bildschirmsperren und Crypto-Ransomware. Wie der Name schon sagt, ist die Bildschirmsperre darauf ausgelegt, dass der Anwender den Computer nicht mehr nutzen kann. Es wird stattdessen eine Aufforderung zur Eingabe eines Kennworts angezeigt. Der Anwender muss den richtigen Code zum Entsperren kaufen, damit die Meldung verschwindet. Diese vor ein paar Jahren noch sehr beliebte Ransomware wurde inzwischen fast vollständig von Crypto-Ransomware ersetzt. Der bösartige Bruder sperrt den Computer nicht, sondern hindert Sie am Zugriff auf Ihre wertvollen Informationen und Erinnerungen, indem er Ihre Dateien verschlüsselt.*
>
> *Die Idee für Ransomware ist an sich nicht sonderlich neu. Bereits 1989, als Heimcomputer noch in den Kinderschuhen steckten, wurde mit dem „AIDS“-Trojaner erstmalig eine Ransomware dokumentiert. „AIDS“ verschlüsselte auf dem Computer die Dateinamen. Um das System dann wieder nutzbar zu machen, musste ein Lösegeld von 189 USD gezahlt werden. Der Urheber der Malware war damals schnell gefunden. Da das Geld von den Opfern nur per Überweisung oder Post gezahlt werden konnte, gab es eine leicht zu verfolgende Spur. Mit dem Erfolg und der weitreichenden Verbreitung anonymer Währungen wie Bitcoin ist es nahezu unmöglich, das Geld aufzuspüren. Dadurch können Ransomware-Banden oftmals Jahre lang im Schatten agieren, ohne gefasst zu werden.*
>
> *Sollte eine Crypto-Ransomware auf Ihr System gelangen, sucht sie nach „interessanten“ Dateien, wie Bilder, Videos, Musik, Speicherstände von Spielen, Datenbanken oder Dokumente. Diese werden dann mithilfe einer Kryptografie*

> *verschlüsselt. Die Art der dazu eingesetzten Verschlüsselung variiert stark. Von einfach zu knackenden, selbst erstellten Algorithmen bis hin zu Codes auf Militärniveau ist alles dabei. Nachdem alle Dateien verschlüsselt wurden, werden meistens auch die Sicherungen und Schattenkopien Ihrer Dateien gelöscht. Zu guter Letzt werden auf dem gesamten Computer Meldungen hinterlassen, die Sie unübersehbar über den soeben durchgeführten Vorgang informieren. Sie beschreiben Ihnen auch, wie Sie das Lösegeld zahlen müssen, um Ihre Dateien wiederzubekommen.*

Weitere Information finden Sie hier:

Angriffe verhindern und bearbeiten
Falls Sie sich gegen Ransomware schützen wollen, bieten wie Ihnen effektive Lösungen an.

Möchten Sie den Angriffen auf Ihren Computer vorbeugen? Wir helfen Ihnen! Schauen Sie hier

Haben Sie eine Anfrage an uns? Senden Sie uns eine Anfrage oder nehen Sie mit uns Kontakt auf: https://nicos-edvdienst.de/kontakt/