**Ransomware**

Eine Ransomware-Attacke ist ein Cyberangriff, bei dem ein Angreifer schädliche Software auf das System eines Opfers einschleust, um dessen Daten und Systeme zu verschlüsseln und unzugänglich zu machen. Der Angreifer fordert dann ein Lösegeld vom Opfer, um die Daten wiederherzustellen und den Zugriff auf das System wiederherzustellen.

Die Ransomware kann auf verschiedene Arten in das System des Opfers eindringen, wie z.B. durch E-Mail-Anhänge, infizierte Websites, Social Engineering oder Schwachstellen in Software und Systemen. Sobald die Ransomware in das System eindringt, beginnt sie, die Daten des Opfers zu verschlüsseln, so dass der Opfer keinen Zugriff mehr darauf hat.

Die Ransomware verwendet in der Regel einen starken Verschlüsselungsalgorithmus, der es nahezu unmöglich macht, die verschlüsselten Daten, ohne den richtigen Entschlüsselungsschlüssel wiederherzustellen. Der Angreifer fordert dann ein Lösegeld, um den Entschlüsselungsschlüssel zu erhalten und den Zugriff auf die Daten wiederherzustellen.

Die Opfer haben oft nur wenige Optionen, wenn sie von einer Ransomware-Attacke betroffen sind. Sie können das Lösegeld zahlen, um den Zugriff auf ihre Daten wiederherzustellen, oder sie können versuchen, ihre Daten aus Backups wiederherzustellen oder die Hilfe von Experten in Anspruch nehmen.

Ransomware-Attacken können schwerwiegende Auswirkungen haben, insbesondere im Gesundheitswesen, da hier sehr sensible Patientendaten betroffen sein können. Es ist daher wichtig, regelmäßige Backups zu erstellen, Sicherheitslücken in Software und Systemen zu minimieren und Mitarbeiter über die Risiken und Folgen von Ransomware-Attacken zu schulen, um das Risiko von Angriffen zu minimieren.

**Einfache und simple Definition:**

Eine Ransomware-Attacke ist ein Angriff auf ein Computersystem, bei dem Schadsoftware verwendet wird, um Daten des Opfers zu verschlüsseln und unzugänglich zu machen. Der Angreifer fordert dann ein Lösegeld, um den Zugriff auf die Daten wiederherzustellen.

**Was machen, wenn sowas passiert:**

Im Falle einer Ransomware-Attacke auf eine Gesundheitsorganisation sollte dieser folgende Schritt unternehmen:

* Sofortige Trennung des betroffenen Netzwerks vom Internet und von anderen Netzwerken, um eine Ausbreitung der Ransomware auf andere Systeme zu verhindern.
* Benachrichtigung der IT-Abteilung und des IT-Sicherheitsbeauftragten, um die Situation schnell zu analysieren und geeignete Maßnahmen zur Eindämmung der Infektion zu ergreifen.
* Sicherung von wichtigen Daten und Systemen, um Datenverluste zu minimieren.
* Einrichtung eines Notfallteams, das sich mit der Ransomware-Attacke befasst und Maßnahmen zur Wiederherstellung der Systeme und Daten koordiniert.
* Erstellung von Backups von kritischen Daten und Systemen, um eine schnelle Wiederherstellung der Systeme zu ermöglichen.
* Analyse der Ransomware und der Art des Angriffs, um geeignete Gegenmaßnahmen zu ergreifen.
* Entfernung der Ransomware von den betroffenen Systemen und Netzwerken.
* Meldung des Vorfalls an die zuständige Aufsichtsbehörde und an die betroffenen Patienten, sofern personenbezogene Daten betroffen sind.
* Implementierung von Maßnahmen, um zukünftige Ransomware-Attacken zu verhindern, wie z.B. regelmäßige Backups, Aktualisierung von Systemen und Software, Schulung von Mitarbeitern im Umgang mit Ransomware-Attacken, etc.

Eine schnelle Reaktion auf eine Ransomware-Attacke ist entscheidend, um den Schaden zu minimieren und eine schnelle Wiederherstellung der betroffenen Systeme und Daten zu ermöglichen.

**Was tun, wenn man kein Backup hat, oder keine Möglichkeit hat es zu umgehen?**

Wenn es kein Backup gibt, dann wird es schwieriger, die Daten wiederherzustellen, nachdem eine Ransomware-Attacke stattgefunden hat. Hier sind einige Optionen, die in Betracht gezogen werden können:

* Zahlung des Lösegeldes: Die Angreifer fordern normalerweise ein Lösegeld, um die verschlüsselten Daten wieder freizugeben. Es gibt jedoch keine Garantie dafür, dass die Angreifer tatsächlich die Daten wiederherstellen, nachdem das Lösegeld gezahlt wurde. Darüber hinaus kann das Zahlen des Lösegeldes als Anreiz für die Angreifer dienen, weitere Ransomware-Attacken durchzuführen.
* Verwendung von Entschlüsselungs-Tools: Es gibt einige Entschlüsselungs-Tools, die kostenlos oder gegen eine Gebühr verfügbar sind. Diese Tools können jedoch nicht für alle Arten von Ransomware und Verschlüsselungsalgorithmen geeignet sein und möglicherweise nicht in der Lage sein, alle Daten wiederherzustellen.
* Wiederherstellung von Daten aus Schattenkopien: Einige Betriebssysteme erstellen automatisch Schattenkopien von Dateien, die als Teil der Systemwiederherstellung gespeichert werden. Diese Schattenkopien können verwendet werden, um ältere Versionen der Dateien wiederherzustellen, bevor sie durch die Ransomware verschlüsselt wurden.
* Expertenhilfe: Es kann sinnvoll sein, sich an einen IT-Sicherheitsexperten oder ein spezialisiertes Unternehmen zu wenden, um bei der Wiederherstellung der Daten zu helfen. Solche Experten können in der Lage sein, die Ransomware zu identifizieren und Maßnahmen zu ergreifen, um die verschlüsselten Daten wiederherzustellen.

Es ist wichtig zu beachten, dass es keine Garantie gibt, dass die Daten wiederhergestellt werden können, nachdem eine Ransomware-Attacke stattgefunden hat, insbesondere wenn kein Backup verfügbar ist. Es ist daher ratsam, regelmäßig Backups zu erstellen und andere Präventivmaßnahmen zu ergreifen, um die Auswirkungen von Ransomware-Attacken zu minimieren.

**Weiteres zu beachten:**

* Keine Zahlung des Lösegelds: Es wird empfohlen, das Lösegeld nicht zu zahlen, da dies die Angreifer ermutigen kann, weitere Angriffe durchzuführen. Darüber hinaus gibt es keine Garantie dafür, dass die Angreifer tatsächlich die Daten wiederherstellen, nachdem das Lösegeld gezahlt wurde.
* Schnelle Reaktion: Eine schnelle Reaktion auf einen Ransomware-Angriff ist entscheidend, um den Schaden zu minimieren und eine schnelle Wiederherstellung der betroffenen Systeme und Daten zu ermöglichen. Daher sollten Unternehmen und Organisationen einen Notfallplan für Ransomware-Attacken haben und sicherstellen, dass Mitarbeiter entsprechend geschult sind.
* Sicherheitsvorkehrungen: Es ist wichtig, Sicherheitsvorkehrungen zu treffen, um das Risiko von Ransomware-Attacken zu minimieren. Dazu gehört die Verwendung von Anti-Viren-Software und Firewalls, regelmäßige Updates von Betriebssystemen und Anwendungen, die Einschränkung von Berechtigungen für Mitarbeiter und die Schulung von Mitarbeitern im Umgang mit verdächtigen E-Mails und Anhängen.
* Backups: Es ist ratsam, regelmäßige Backups von wichtigen Daten zu erstellen und sicherzustellen, dass diese Backups an einem sicheren Ort gespeichert werden. Wenn eine Ransomware-Attacke stattfindet, können Backups verwendet werden, um die Daten schnell wiederherzustellen und die Auswirkungen des Angriffs zu minimieren.

Es ist wichtig zu beachten, dass Ransomware-Attacken sehr ernst sind und eine erhebliche Bedrohung für Unternehmen und Organisationen darstellen. Eine schnelle Reaktion, eine angemessene Schulung der Mitarbeiter und die Umsetzung geeigneter Sicherheitsvorkehrungen können jedoch dazu beitragen, das Risiko von Angriffen zu minimieren und den Schaden zu begrenzen.