Ransomware: Eine Bedrohung erklärt

Ransomware ist eine Bedrohung, die sich rasch zu einem ernsten Problem entwickelt, das von der gesamten Welt wahrgenommen wird. In dieser Schlüsselinformation wird ein Einblick in die Gestalt und Funktionsweise von Ransomware gegeben, was bisherige Beispiele betrifft und was am besten gemacht werden kann, um sich selbst vor einem solchen Angriff zu schützen.

Was ist Ransomware?

Ransomware ist ein Programm, das in den Computer eines bestimmten Benutzers eindringt und dann den gesamten Inhalt verschlüsselt. Diese Art von Schad-Software stiehlt den Benutzern normalerweise ihre Daten und verweigert ihnen den Zugriff darauf, bis ein Lösegeld gezahlt wird. Der Entwickler der Software begeht diese Tat, weil er damit Erpressungsgelder verdienen möchte.

Ransomware ist eine der komplexesten Arten von Malware. Es hat sich zu einem globalen Problem entwickelt, da viele böswillige Individuen immer mehr auf die Idee kommen, diese Art von Schadsoftware zu verwenden, um ihren finanziellen Nutzen aus Unternehmen und Privatpersonen herauszuholen.

Es hat sich gezeigt, dass die Fähigkeiten des Ransomwares sich ständig verbessern, da es immer mehr Erpressungsgelder ausnutzt.

Wie funktioniert Ransomware?

Ransomware funktioniert, indem böswillige Software den Zugriff des Benutzers auf seine Computerdaten blockiert oder verweigert und den Benutzer dazu zwingt, ein Lösegeld zu zahlen, damit er wieder Zugang zu seinen Daten erhält. Diese Software greift in der Regel auf verschiedene Arten von Programmen oder Dateien zu, die einige Art von Wert für den

Angreifer haben. Wenn die Software den Zugriff darauf blockiert, wird der Benutzer dazu gezwungen, das Lösegeld zu zahlen, wenn er wieder Zugriff auf seine Dateien erhalten möchte.

Die Erpresser versuchen normalerweise, das Lösegeld in Form von Bitcoins oder anderer anonymisierter Zahlungsweisen einzufordern, um ihre Identität zu schützen. Es ist nicht ungewöhnlich, dass Erpresser ihre Opfer für weitere Lösegelder verfolgen, nachdem sie das ursprüngliche Lösegeld erhalten haben.

Ransomware kann über eine Reihe verschiedener Techniken verbreitet werden, wie z.B. E-Mail-Anhänge, böswillige Software, die als harmlose Anwendung getarnt ist oder über öffentliche Wi-Fi-Netzwerke. Wenn die Software erfolgreich installiert wurde, kann sie in der Regel direkt beginnen, ihr Ziel zu erreichen: es verschlüsselt alle Daten, die der Benutzer auf seinem Computer gespeichert hat, und blockiert den Zugriff darauf.

Chronologie und Beispiele von Ransomware-Angriffen

Die erste Ransomware-Malware-Infektion wurde 1989 mit dem Namen “AIDS-Trojaner” eingeführt. Seitdem hat sich die Malware weiterentwickelt und immer mehr Unternehmen, Organisationen und sogar Regierungen auf der ganzen Welt betroffen. Einige der berühmtesten Ransomware-Attacken in den letzten Jahren waren:

- WannaCry (2017): Dieser Ransomware-Angriff hat 130.000 Computer in 150 Ländern infiziert.
- NotPetya (2017): Dieser Angriff hat mehr als 1.000 Unternehmen infiziert und im selben Jahr 1,2 Milliarden USD an Erpressungsgeldern eingefordert.
- Bad Rabbit (2017): Dieser Angriff hat 250.000 Computer in Ost- und Südeuropa infiziert.

Wie kann man sich vor Ransomware schützen?

Es gibt einige einfache Schritte, die Unternehmen und Privatpersonen ergreifen können, um sich vor Ransomware-Angriffen zu schützen. Dazu gehören:

- Ständige Aktualisierung der Software und des Betriebssystems: Es ist sehr wichtig, dass alle Software- und Betriebssystem-Updates befolgt werden, da diese häufig neue Sicherheitslücken verhindern und beheben.
- Verwendung eines Firewalls und eines Virenschutzprogramms: Ein Firewall kann helfen, böswillige Viren abzuwehren, während ein Virenschutzprogramm versucht, eindringende Schadsoftware zu erkennen und zu entfernen.
- Vermeiden des Besuchs unprofessioneller oder böswilliger Websites: Der Besuch böswilliger oder unprofessioneller Websites kann dazu führen, dass Ransomware auf das Gerät heruntergeladen wird.
- Verwendung der bevorzugten Sicherheits- und Datensicherungslösungen: Ein Unternehmen sollte sicherstellen, dass es die datensichersten Lösungen verwendet, um sicherzustellen, dass alle Daten gesichert und verschlüsselt sind.

Schlussfolgerung: Die Bedrohung durch Ransomware

Ransomware ist ein globaler Bedrohungstyp, der milliardenschwere Kosten, finanzielle Verluste und immense Unannehmlichkeiten mit sich bringen kann. Es ist wichtig zu wissen, wie und wo Ransomware entsteht und wie man sich selbst und sein Unternehmen vor einem solchen Angriff schützen kann. Mit der richtigen Technologie und dem richtigen Wissen können Unternehmen und Individuen auf die Gefahren von Ransomware vorbereitet sein und somit die Wahrscheinlichkeit eines erfolgreichen Angriffs erheblich reduzieren.

In den letzten Jahren sind wir Zeugen der verbesserten Fähigkeiten der Ransomware geworden. Viele bösartige Individuen haben versucht, ihren finanziellen Nutzen auf Kosten anderer zu suchen und es ist unerlässlich, dass sowohl Unternehmen als auch Privatpersonen die neuesten Technologien verwenden, um sich effektiv vor Ransomware-Angriffen zu

schützen.

Wie hilfreich war dieser Beitrag?

Klicke auf die Sterne um zu bewerten!

Bewertung Abschicken
Durchschnittliche Bewertung / 5. Anzahl Bewertungen:

Top-Schlagwörter: Infektion, Wahrscheinlichkeit, Lösegeld, Bad Rabbit, Betriebssystem, Ziel, Wissen, Problem, Computer, Daten

Verwandte Artikel

- Schützen Sie Ihr Unternehmen mit Cybersecurity
- Effektiver Virenschutz: Tipps für sicheres Surfen
- Wie führe ich eine CAFM-Software in meinem Unternehmen ein?