Whitepaper 08/2023

Leitfaden bei einer Ransomware-Attacke

Ransomware-Angriffe sind eine wachsende Bedrohung für Unternehmen aller Größen und Branchen. Sie können erhebliche Schäden verursachen und den Betrieb erheblich stören.

Dieser Leitfaden bietet erste Hilfestellungen, wie man auf einen Ransomware-Angriff reagieren sollte.

Was ist Ransomware?

Ransomware ist eine Art von Malware, die Dateien auf einem Computer oder Netzwerk verschlüsselt und dann ein Lösegeld für deren Entschlüsselung verlangt. Die Angriffe sind oft sehr gezielt und koordiniert, und die Angreifer nutzen verschiedene Einfallstore, um Malware-Codes in ein System oder Netzwerk einzuschleusen. Diese Einfallstore können E-Mails mit kompromittierten Anhängen oder Links zu bösartigen Websites sein. Die Angreifer können auch bekannte Sicherheitslücken in Software oder Betriebssystemen ausnutzen.

Was tun, wenn Sie angegriffen wurden?

- **Isolieren Sie das betroffene System:** Sobald Sie feststellen, dass Sie angegriffen wurden, sollten Sie das betroffene System so schnell wie möglich vom Netzwerk isolieren, um zu verhindern, dass sich die Ransomware weiter ausbreitet.

- **Verstehen Sie den Angriffsvektor:** Es ist wichtig zu verstehen, wie der Angriff stattgefunden hat. Dies hilft Ihnen, den Vorfall zu bewältigen und wertvolle Lektionen für die Zukunft zu ziehen.

- **Sichern und überprüfen Sie Ihre Backups:** Backups sind unerlässlich, um Ihre Daten wiederherzustellen. Stellen Sie sicher, dass Ihre Backups sicher sind und nicht von der Ransomware betroffen sind.

- **Ändern Sie Ihre Passwörter:** Es ist immer eine gute Idee, die Passwörter systemkritischer Nutzerkonten zu ändern, um sicherzustellen, dass der Angreifer keinen weiteren Zugriff auf Ihr System hat.

Wie können Sie sich vor Ransomware-Angriffen schützen?

Es gibt mehrere Maßnahmen, die Sie ergreifen können, um Ihr Unternehmen vor Ransomware-Angriffen zu schützen:

- **Bewusstsein schaffen**: Schulen Sie Ihre Mitarbeiter im sicheren Umgang mit IT und Unternehmensdaten. Sie sollten in der Lage sein, potenzielle Bedrohungen zu erkennen und zu wissen, wie sie darauf reagieren sollten.

- **Patch Management**: Halten Sie Ihre Software und Betriebssysteme immer auf dem neuesten Stand. Überprüfen Sie regelmäßig CVEs (Common Vulnerabilities and Exposures), um Schwachstellen in Ihrem System zu identifizieren und zu beheben.

- **Netzwerksegmentierung**: Durch die Trennung von Servern, Clients und Produktionsnetzen können Sie verhindern, dass sich Schadsoftware auf weitere Systeme ausbreitet.

- **Implementieren Sie ein Zero-Trust-Konzept**: Bei einem Zero-Trust-Konzept wird grundsätzlich keinem Benutzer oder System vertraut. Jeder Zugriff muss explizit genehmigt werden, und alle Benutzer und Systeme müssen sich authentifizieren.

- **Erstellen Sie ein Notfallhandbuch und ein Business Continuity Management (BCM)**: Diese geben Ihnen einen Schritt-für-Schritt-Rahmen an die Hand, um sich optimal auf Angriffe und Ausfälle in der IT-Infrastruktur vorzubereiten.

Sie brauchen Unterstützung?

Unser Team aus zertifizierten IT-Sicherheitsexperten steht bereit, um Sie sowohl bei der Bewältigung eines aktuellen Angriffs als auch bei der Prävention zukünftiger Angriffe zu unterstützen.

Wir verstehen, dass jede Minute zählt, wenn Sie unter einem Angriff stehen. Unsere Experten können schnell und effizient handeln, um Ihre Systeme zu sichern, den Schaden zu minimieren und die Wiederherstellung Ihrer Daten zu unterstützen.

Alle Informationen und unsere Kontaktdaten finden Sie unter:

www.gallwitz-its.de/informationssicherheit

Unsere Partner für Ihre Sicherheit

SentinelOne

ENGAGE
FORTINET ADVOCATE PARTNER
Integrator

Sophos
Authorized
Partner