SRB
Assekuranz Broker AG

Newsletter - Cyber Sicherheitshinweis

Gerne informieren wir Sie, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) folgende Meldung zu **Emotet** inkl. Information zur Angriffsmethode veröffentlicht hat:

- Gefälschte E-Mails im Namen von Kollegen, Geschäftspartnern oder Bekannten

- Durch das sogenannte "Outlook-Harvesting" ist Emotet in der Lage, authentisch aussehende Spam-Mails zu verschicken. Dazu liest die Schadsoftware Kontaktbeziehungen und seit einigen Wochen auch E-Mail-Inhalte aus den Postfächern bereits infizierter Systeme aus.

- Diese Informationen nutzen die Täter zur weiteren Verbreitung des Schadprogramms in nachfolgenden Spam-Kampagnen, so dass die Empfänger fingierte Mails von Absendern erhalten, mit denen sie erst kürzlich in Kontakt standen.

- Das BSI rechnet daher künftig mit einer weiteren Zunahme an gut gemachten, automatisierten Social-Engineering-Angriffen dieser Art, die für die Empfänger kaum noch als solche zu identifizieren sind.

- Diese Methode eignet sich ebenfalls zum Einsatz von hochspezialisierten Spear-Phishing-Angriffen auf besonders hochwertige Ziele.

Info vom BSI

Diese Ransomware treten in den Varianten „Ryuk" und „Emotet" auf und werden derzeit als die weltweit gefährlichsten Bedrohungen mittels Schadsoftware u.a. durch das Bundesamt für Sicherheit in der Informationstechnik BSI eingestuft.

Die aktuellen Kampagnen sind von der Angriffsphase bis zum Verschlüsselungsprozess und der eigentlichen Lösegeldforderung sehr sorgfältig umgesetzt und v.a. gegen Unternehmen ausgerichtet, die in der Lage sind, viel Geld zu bezahlen, um den reibungslosen Geschäftsbetrieb wieder aufnehmen zu können.

Die Angriffe sind sehr zielgerichtet und per E-Mail werden betroffene Unternehmen aufgefordert, hohe Summen in Bitcoin zu bezahlen, um den Entschlüsselungs-Code zu erhalten. Die Schadprogramme werden aufgrund ständiger Modifikationen zunächst meist nicht von gängigen Virenschutzprogrammen erkannt und nehmen tiefgreifende Änderungen an infizierten Systemen vor. Bereinigungsversuche bleiben in der Regel erfolglos und bergen die Gefahr, dass Teile der Schadsoftware auf dem System verbleiben. In jedem betroffenen Fall sind Server inklusive der Back-Up Server verschlüsselt gewesen. Infizierte Systeme

gelten daher als vollständig kompromittiert und müssen neu aufgesetzt werden, so dass es hierdurch dann in den betroffenen Firmen zu Produktionsausfällen gekommen ist.

Cyber-Crime Zahlen und Informationen

Bei dieser Gelegenheit möchten wir Sie über die aktuellen Cyber-Crime Zahlen und Informationen informieren. Der nachfolgende Link führt Sie zu einem interessanten Artikel zu diesem Thema:

Informationen

Das wichtigste in Kürze:

Zusammenfassung

Unsere Kundenbetreuer stehen Ihnen für weitere Auskünfte gerne zur Verfügung.

Freundliche Grüsse

SRB Assekuranz Broker AG

Luggwegstrasse 9, Postfach, CH-8048 Zürich
Telefon: + 41 44 497 87 87
Fax: + 41 44 497 87 88
info@srb.ch, www.srb.ch

Brokerslink Partner