Warnung vor der Verschlüsselungssoftware „Cerber“!

Art der Bedrohung: Ransomware
Ransomware ist ein Überbegriff für Schadsoftware, die dazu dient, Computer und Daten zu verschlüsseln und als „Geiseln“ zu nehmen. Für die Entschlüsselung wird von den Tätern Lösegeld (engl. ransom) gefordert.

Erstmaliges Auftreten
März 2016 / Österreich: Mai 2016

Modus Operandi
Cyberkriminelle verbreiten Ransomware durch manipulierte Email-Anhänge, durch Ausnützen bestehender Sicherheitslücken sowie durch unbeabsichtigtes Herunterladen aus dem Internet (drive-by-download). Sobald ein System infiziert ist, werden darauf befindliche Daten verschlüsselt und somit unbrauchbar gemacht. Die Verschlüsselung erstreckt sich auf verbundene Datenträger ebenso wie auf Netzlaufwerke. Neben den verschlüsselten Daten bleibt ein „Erpresserschreiben“ zurück, dem eine Anleitung zum Bezahlen des Lösegeldes sowie zum Wiederherstellen der Daten zu entnehmen ist.
Die Ransomware „Cerber“ wird aktuell durch gefälschte Bewerbungsschreiben verbreitet. Die Täter antworten auf Stellenangebote im Internet und versenden den Schadcode mit den beigefügten Dateien, die beispielsweise als Lebenslauf getarnt sind. Dadurch verleihen sie ihren Emails eine erhöhte Plausibilität und Glaubwürdigkeit. Beim Öffnen der Datei wird der Schadcode ausgeführt bzw. aus dem Internet nachgeladen. In weiterer Folge werden Daten auf sämtlichen im Netzwerk befindlichen Computern und Laufwerken verschlüsselt.

Empfehlungen
Zur Minimierung des Risikos:
- Führen Sie regelmäßig Backups durch und trennen Sie diese physisch vom Netz (abstecken)
- Deaktivieren Sie Makros in Office-Anwendungen
- Deaktivieren Sie den Windows Script Host
- Blockieren Sie Programme aus den %LocalAppData% und %AppData% Ordnern
- Aktivieren Sie die Anzeige von Dateierweiterungen, auch von bekannten Dateitypen, um getarnte Dateien zu entlarven (z.B. „Kein-Virus.pdf.exe“)
- Stellen Sie für „risikobehaftete“ Dateierweiterungen (.js, .doc, etc.) das Standardprogramm zum Öffnen um auf „Editor“ oder „Notepad“
- Aktivieren Sie Ihre Firewall
- Aktivieren Sie Software zur Kontrolle der Ausführung von Programmen
- Schränken Sie Benutzerrechte ein (Ransomware kann nur jene Dateien verschlüsseln, auf die sie auch Schreibrechte hat)
- Beurteilen Sie insgesamt die Plausibilität und Glaubwürdigkeit von Email-Nachrichten bevor Sie Dateien öffnen

Vorgehen im Schadensfall:

- Trennen Sie die betroffenen Geräte vom Netz und schalten Sie diese aus
- Erstatten Sie umgehend Anzeige auf der nächsten Polizeidienststelle
- Für weitere Informationen kontaktieren Sie die Cybercrime-Meldestelle im Bundeskriminalamt: Tel (24h): +43-1-24836-986500; Email: against-cybercrime@bmi.gv.at

Beispiel für ein verwendetes Bewerbungsschreiben

- Texte werden zwecks Massenaussendung sehr allgemein formuliert

Sehr geehrte Damen und Herren,

anbei erhalten Sie meine Bewerbung für Ihre im Internet ausgeschriebene Stelle. Warum ich die Stelle optimal ausfüllen kann und Ihrem Unternehmen durch meine Erfahrung zahlreiche Vorteile biete, entnehmen Sie bitte meinen ausführlichen und angehängten Bewerbungsunterlagen.

Ich freue mich, wenn ich mich Ihnen noch einmal persönlich vorstellen kann.

Mit freundlichen Grüßen,

[redacted]

HERAUSGEBER: Bundesministerium für Inneres
Bundeskriminalamt
A-1090 Wien, Josef Holaubek Platz 1
Tel.: +43 1 24836 986500

FEEDBACK

NEWSLETTER AN-/ABMELDUNG