Niedersächsisches Ministerium
für Inneres und Sport

Wirtschaftsschutz - *Info*

Hannover, im Februar 2016

Sehr geehrte Damen und Herren,

betriebliche Daten, welche auf IT-Systemen gespeichert werden, sind einer immer größeren Bedrohung durch eine Vielzahl von Angreifern und Angriffswegen ausgesetzt.

Aus gegebenem Anlass möchten wir Ihnen Informationen zum Themenfeld Schutz von digitalen Daten anbieten, da dem niedersächsischen Wirtschaftsschutz vermehrt von Unternehmen Angriffe auf die Integrität von gespeicherten Daten durch Verschlüsselungstrojaner gemeldet werden.

Es zeigt sich hier, wie wichtig es ist, auch im Bereich des Datenbackups eine stringente Sicherheitsstrategie zu fahren.

Für Rückfragen zu diesem Thema stehen wir jederzeit gerne zur Verfügung, wobei das Angebot des Wirtschaftsschutzes zu individuellen und vertraulichen Gesprächen unberührt bleibt.

Ihr Wirtschaftsschutz-Team

Niedersächsische Verfassungsschutzbehörde

Niedersächsisches Ministerium für Inneres und Sport
Referat 55 - Wirtschaftsschutz

Postfach 4420
30044 Hannover
Tel.: 0511 / 6709-247 oder -248
Email: wirtschaftsschutz@verfassungsschutz.niedersachsen.de

Falldarstellung

In letzter Zeit werden an Personalstellen in Unternehmen personalisierte Bewerbungen auf ausgeschriebene Stelle per E-Mail gesandt, welche die eigentlichen Bewerbungsunterlagen als Downloadlink über den Onlinespeicherdienst Dropbox anbieten. Ein Klick auf den Link startet den Download einer Schadsoftware (Ransomware[1]), die sich dann oft zunächst unbemerkt im Hintergrund installiert. Dieser Verbreitungsweg ist relativ neu und den personalbearbeitenden Stellen in Unternehmen in der Regel nicht bekannt. Bisher wurde diese Art von Schadsoftware über infizierte E-Mail Anhänge und über präparierte Webseiten, so genannte Drive-By-Downloads, verbreitet.
Nach Installation verschlüsselt die Schadsoftware die Dateien, welche sich auf dem Computer des Anwenders befinden (beispielsweise Excel- oder Word-Dateien). Es sind auch Fälle bekannt, in denen eingebundene Netzlaufwerke ebenfalls verschlüsselt wurden.
Verschiedene Antiviren-Produkte können die Schadsoftware entdecken und löschen, dann ist es aber meistens zu spät, weil die auf dem Computer vorhandenen Dateien bereits verschlüsselt wurden. In diesem Fall ist deshalb nicht die Entfernung der Schadsoftware das Problem, sondern die Wiederherstellung der ursprünglichen Daten.

Wie können Sie sich schützen:

- Auf dem Computer abgelegte Daten sollten regelmäßig auf externe Datenträger kopiert werden (Backup). Diese sollten **nur** während des Backupvorgangs am Computer angeschlossen sein.
- Sowohl Betriebssystem als auch installierte Applikationen (z.B. Adobe Reader, Adobe Flash, Sun Java etc.) müssen immer auf den neuesten Stand gebracht werden. Falls vorhanden, am besten mit der automatischen Update Funktion.

[1] Ransomware sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt, welche aufgehoben werden soll durch Zahlung von "Lösegeld".

- Ein Antivirenprogramm muss installiert und auf dem neusten Stand sein.
- Eine Personal Firewall muss installiert und auf dem neusten Stand sein.
- Seien Sie immer vorsichtig bei verdächtigen E-Mails, bei E-Mails, welche Sie unerwartet bekommen, oder welche von einem unbekannten Absender stammen! Befolgen Sie hier keine Anweisungen im Text, öffnen Sie keinen Anhang und folgen Sie keinen Links!
- Müssen E-Mails dieser Art bearbeitet werden, verwenden Sie einen Stand-Alone-Rechner, welcher nicht an das Unternehmensnetz angebunden ist und auf dem sich keine relevanten Daten befinden!

Sollten Sie bereits Opfer von Verschlüsselungstrojanern sein:

Für Opfer von TeslaCrypt ist die Software TeslaDecoder[2] kostenfrei verfügbar, welche mit TeslaCrypt, bis zur Version 2.2.0, verschlüsselte Dateien mit den Endungen .aaa, .abc, .ccc, .ecc, .exx, .vvv, .xyz und .zzz entschlüsselt.

Für andere Verschlüsselungstrojaner wie Chimera oder Cryptowall 3.0 steht z.Z. leider keine Entschlüsselungshilfe zur Verfügung.

Interessante Links in anderer Sache:

Verfassungsschutz veröffentlicht neue Broschüren zum Salafismus
http://www.verfassungsschutz.niedersachsen.de/portal/live.php?navigation_id=12260&article_id=140557&_psmand=30

Spionage - (k)ein Thema?!
http://www.verfassungsschutz.niedersachsen.de/portal/live.php?navigation_id=12264&article_id=140631&_psmand=30

[2] http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/