POLIZEI
Nordrhein-Westfalen
Düsseldorf

bürgerorientiert · professionell · rechtsstaatlich

Präventionshinweis Cybercrime

Thema: Bewerbungsmail mit Schadsoftware im Anhang

Immer wieder werden Firmen per E-Mail mit Bewerbungen von Jobsuchenden angeschrieben. Das ist in der heutigen Zeit durchaus üblich – und genau hierauf zielen Täter ab. Statt einer Bewerbung enthalten diese Mails Schadsoftware, welche dann durch Mitarbeiter/innen mit Zugang zum Mailkonto ungewollt installiert wird.

Personalabteilungen, aber auch normale Mitarbeiter/innen in Firmen und Vereinen, werden von Jobsuchenden per E-Mail angeschrieben. Die Betreffzeile der E-Mail lautet dann beispielsweise „Bewerbung auf die von Ihnen ausgeschriebene Stelle“, teilweise auch in Kombination mit einem erfundenen Namen.

In der Mail selbst schreiben die Täter einen kurzen Begrüßungstext und fügen ein Portraitfoto einer jungen Frau, welches meist von einer fremden Webseite stammt, hinzu. Für weitere Informationen wird auf den Dateianhang verwiesen, welcher meist eine komprimierte Datei im ZIP-Format („ZIP-Archiv“) enthält. Diese kann in den aktuellen Windows-Versionen ohne zusätzliche Software per Doppelklick geöffnet werden. In dem Archiv befinden sich zumeist Dateien wie z.B. „Lebenslauf.pdf.exe“. Da durch die Standardeinstellungen von Windows die letzte Dateiendung unterdrückt wird, zeigt der Dateiexplorer nur „Lebenslauf.pdf“ an. Wer nun in dem Glauben, es würde sich um eine PDF-Datei handeln, diese Datei anklickt, startet in Wirklichkeit die Schadsoftware. Die Dateien auf dem Computer und allen eventuell verbundenen Netzwerklaufwerken werden dann verschlüsselt. Auf dem Bildschirm erscheint eine Meldung, mit der eine Bitcoin-Zahlung erpresst wird.

Bisher erkennen leider noch nicht alle Antivirenprogramme die Schadsoftware. Eine Überprüfung mit einer anerkannten Virusprüfseite ergab, dass derzeit (April 2019) nur 26 von 65 verfügbaren Programmen die Gefahr erkennen.

Wichtig ist die Schulung der Mitarbeiter/innen in Unternehmen. Es müssen Vorkehrungen getroffen werden, solche Mails auf gefährliche Inhalte zu prüfen, z. B. mit einem alternativen Betriebssystem oder zumindest durch Ändern der Anzeigeeinstellungen im Datei-Explorer.

Sollten Sie den Anhang bereits ausgeführt und somit Ihr Computersystem geschädigt haben, so raten wir dazu, die geforderte Zahlung nicht zu tätigen. Trennen Sie den betroffenen Computer sofort vom Netzwerk und erstatten Sie Anzeige.

Informationen zu Ransomware bzw. Cryptotrojanern finden Sie hier: **www.botfrei.de**

KK KP/O 2019