Baden-Württemberg
LANDESKRIMINALAMT

Warnmeldung für Firmen

Stuttgart, 24.03.2016

Falsche Bewerbung 2.0: Digitale Erpresser verstecken wieder Schadsoftware in Bewerbungsschreiben

Dem Landeskriminalamt Baden-Württemberg (LKA BW) liegen seit dem 24.03.2016 aktuelle Hinweise vor, dass Kriminelle erneut potentielle Arbeitgeber ins Visier nehmen. Über die Erpressungsmasche berichtete die Zentrale Ansprechstelle Cybercrime (ZAC) bereits am 20.10.2015:

In einer bundesweiten Welle erhalten Unternehmen aktuell unscheinbare E-Mails von angeblichen Bewerbern, die in einem guten Deutsch verfasst sind. Kriminelle geben sich hier als Bewerber aus und schreiben die Geschäftsführung oder die Personalabteilung des Unternehmens direkt an. Ziel dieser Kriminellen ist es, den Computer der Firma mit einer Schadsoftware zu infizieren, die für eine Verschlüsselung der Firmendaten sorgt. Anschließend fordern sie zur Entschlüsselung dieser Daten ein „Lösegeld“.

Die angeblichen Bewerber erklären der Geschäftsführung, wie sie auf ihr Unternehmen aufmerksam geworden sind und bieten weitere Informationen zu ihrer Person über eine in der E-Mail enthaltene „Dropbox-Verknüpfung“ an. Beim Betätigen dieses Links erfolgt jedoch keineswegs der Download der in Aussicht gestellten Bewerberunterlagen. Vielmehr installiert sich eine Schadsoftware, die unmittelbar mit der Verschlüsselung der Firmendaten auf dem Computer beginnt.

Taubenheimstraße 85 · 70372 Stuttgart · Telefon 0711 5401-0 · Telefax 0711 5401-3355
Stuttgart.lka@polizei.bwl.de · www.lka-bw.de · www.polizei-bw.de

Die derzeit bekannten Fälle weisen große Parallelen zu der Vorgehensweise im Oktober 2015 auf. Die Kriminellen senden ihre gefälschten Bewerbungen wieder direkt an Unternehmen, die tatsächlich vakante Stellen öffentlich ausgeschrieben haben. Sie versuchen die angeschriebenen Personalverantwortlichen dazu zu bringen, eine Datei mit dem Namen **„Bewerbungsmappe-gepackt.exe“** vom Cloud-Speicherdienst Dropbox herunterzuladen. Die Datei liegt den bisherigen Erkenntnissen nach in einem Ordner, der den Namen **„Bewerbungsmappe“** trägt. Hierbei gilt es allerdings zu beachten, dass die Täter den Namen der Datei und des Ordners jederzeit verändern können.

Wenn es den Kriminellen gelungen ist, ein System zu infizieren führt sich die Datei automatisch aus und sperrt die betroffenen Computer. Anstelle des Windowssymbols wird ein Totenkopf anzeigt und der Rechner kann nicht mehr ordnungsgemäß genutzt werden. Die Opfer werden über ein digital hinterlegtes Schreiben aufgefordert über den so genannten „TOR Browser“ Kontakt mit den Tätern aufzunehmen.

Wirtschaftsunternehmen, die aktuell auf der Suche nach neuen Mitarbeiten sind sollten die nachfolgenden Sicherheitshinweise der Polizei dringend beachten:

- Prüfen Sie eingehende E-Mails sorgfältig, insbesondere dann, wenn Sie über einen Link zum Download von Unterlagen unbekannter Quellen aufgefordert werden.
- Achten Sie auf die tatsächliche Dateiendung der Bewerbungsunterlagen.
- Die Endungen .exe oder .js weisen darauf hin, dass es sich um ausführbare Dateien handelt, die gegebenenfalls nicht erwünschte Änderungen am PC vornehmen.
- Gehen Sie nicht auf die Forderung der Kriminellen ein und erstatten Sie Anzeige bei der ZAC.
- Erstellen Sie regelmäßig Backups und bewahren Sie diese auf externen Systemen auf, damit diese nicht auch durch die Schafsoftware verschlüsselt werden.

Taubenheimstraße 85 · 70372 Stuttgart · Telefon 0711 5401-0 · Telefax 0711 5401-3355
Stuttgart.lka@polizei.bwl.de · www.lka-bw.de · www.polizei-bw.de

- Sensibilisieren Sie Ihre Mitarbeiter bzgl. der dargestellten Gefahren.

Zentrale Ansprechstelle Cybercrime
beim Landeskriminalamt Baden-Württemberg.

Die ZAC dient als zentraler Ansprechpartner für die Wirtschaft und Behörden in allen Belangen des Themenfeldes Cybercrime.

Erreichbarkeit der ZAC
Telefon: +49 (0)711 5401 2444
E-Mail: cybercrime@polizei.bwl.de

Taubenheimstraße 85 · 70372 Stuttgart · Telefon 0711 5401-0 · Telefax 0711 5401-3355
Stuttgart.lka@polizei.bwl.de · www.lka-bw.de · www.polizei-bw.de