Niedersächsisches Ministerium
für Inneres und Sport
Verfassungsschutz

Wirtschaftsschutz - *Info*

Hannover, im Dezember 2016

Sehr geehrte Damen und Herren,

aus gegebenem Anlass möchten wir sie auf eine uns von Unternehmen mitgeteilte Variante von **CEO-Fraud Angriffen** in unserer Falldarstellung hinweisen.

Weiterhin möchten wir Sie über eine aktuelle Warnmeldung aus dem Bayerischen Landesamt für Verfassungsschutz informieren.

Infrastruktur und Werkzeuge der Hackergruppe CLEAVER / OILRIG

Angriffsfläche sind hier staatliche Einrichtungen und internationale Industrieunternehmen aus den Branchen Telekommunikation, Finanzen, Luft- und Raumfahrt sowie Petrochemie. Es sind dem Schreiben Indikatoren in Form einer OpenIOC Datei beigelegt. Zusätzlich sind YARA-Regeln zu den Angriffswerkzeugen in der Anlage zu finden.

Selbstverständlich stehen wir bei Rückfragen jederzeit gerne zur Verfügung und halten das Angebot des Wirtschaftsschutzes zu individuellen und vertraulichen Gesprächen aufrecht.

Ihr Wirtschaftsschutz-Team

Niedersächsische Verfassungsschutzbehörde

Niedersächsisches Ministerium für Inneres und Sport
Referat 55 - Wirtschaftsschutz

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

Fallkurzdarstellung

Unbekannte Täter schreiben eine Mitarbeiterin der Buchhaltung im Unternehmen mit gefälschter E-Mail-Adresse des Geschäftsführers an und kündigen den Anruf einer Anwaltskanzlei zum Zwecke einer Firmenübernahme an.

Tatsächlich wird die Mitarbeiterin mit unterdrückter Rufnummer von einer unbekannten Person in aktzentfreiem Hochdeutsch angerufen und für die weiteren Abläufe zur vermeintlichen Firmenübernahme instruiert.

Im Anschluss werden per E-Mail vom angeblichen Geschäftsführer der Mitarbeiterin detaillierte Zahlungsanweisungen übermittelt.

Diese Kombination aus E-Mail und telefonischer Ansprache unter gegenseitiger Integritätsbescheinigung ist noch relativ unbekannt und wird offensichtlich von einem intensiven Social Engineering zu den beteiligten Mitarbeitern und Arbeitsabläufen im betroffenen Unternehmen begleitet.

Sollten Sie durch diesen Angriff bereits geschädigt worden sein und eine Anzeige erstatten wollen, wenden Sie sich bitte an die Polizei unter zac@lka.polizei.niedersachsen.de.

Selbstverständlich stehen auch wir Ihnen unter unseren vorseitig gelisteten Kontaktadressen zur Verfügung.