Niedersächsisches Ministerium
für Inneres und Sport

Wirtschaftsschutz - *Info*

Hannover im August 2015

Sehr geehrte Damen und Herren,

aus gegebenem Anlass möchten wir Ihnen verschiedene aktuelle Fälle mit wirtschaftskriminellem Hintergrund näher bringen, die dem niedersächsischen Wirtschaftsschutz gemeldet wurden.

- Risiken durch externe IT-Dienstleister.
- Fake Boss Angriffe auf Mitarbeiter mit Zahlungsvollmacht.

Selbstverständlich stehen wir bei Rückfragen jederzeit gerne zur Verfügung und auch das Angebot des Wirtschaftsschutzes zu individuellen und vertraulichen Gesprächen bleibt davon unberührt.

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

1. **Risiken durch externe Dienstleister**

Falldarstellung:
Ein leitender Mitarbeiter eines medizinischen Dienstleistungsunternehmens kündigt aus Verärgerung über Kompetenzbeschneidungen in seinem Arbeitsbereich. Im Nachgang gründet er ein eigenes Unternehmen im Wettbewerbsumfeld seines alten Arbeitgebers. Seine Unternehmens-IT wird offensichtlich vom selben Dienstleister betreut, der auch für den ehemaligen Arbeitgeber tätig ist.

Eine Prüfung seines ehemaligen Arbeitsplatz-PC's ergab, dass er Unternehmens-Know-how aus dem Firmen-Netz mit Unterstützung des IT-Dienstleisters nach extern ausgeleitet hatte.

Welche Daten der ehemalige Mitarbeiter aus dem Unternehmen geschleust hat und die Art der Beteiligung des IT-Dienstleisters, ist zurzeit Gegenstand von Ermittlungen.

In diesem Zusammenhang möchten wir Sie auf unsere Handlungsempfehlungen im Newsletter 11/2012 hinweisen, verbunden mit dem Hinweis, dass auch externe Dienstleister in die Verfahrensweise für ausscheidende Mitarbeiter eingebunden werden müssen.

http://www.verfassungsschutz.niedersachsen.de/download/82677/Newsletter_Wirtschaftsschutz_11_2012_-_Know-how-Abfluss_durch_ausscheidende_Mitarbeiter.pdf

2. Fake Boss Angriffe auf Mitarbeiter mit Zahlungsvollmacht

Falldarstellung:

Ein Mitarbeiter des Rechnungswesens eines großen produzierenden Unternehmens bekommt eine E-Mail des Firmenleiters. In dieser Mail wird der Mitarbeiter über Belanglosigkeiten informiert und um Rückantwort gebeten. Nach erfolgter Antwort auf diese Mail kommt eine weitere Email des Geschäftsführers mit dem Auftrag einen hohen sechsstelligen Betrag auf ein Konto in China zu überweisen. In der irrigen Annahme tatsächlich mit dem Vorgesetzten zu kommunizieren wird die Summe anstandslos vom Mitarbeiter transferiert.

Was ist passiert?

Unbekannte Angreifer haben mit einer modifizierten E-Mailadresse (Name_des_Geschäftsführer@provider.com) den Mitarbeiter erfolgreich über die Identität des Kommunikationspartners getäuscht. Zusätzlich wurde die Anzeigeeigenschaft des Mailversenders auf den Vor- und Zuname des Geschäftsführers eingestellt.
Die Antwort des Mitarbeiters über die Antwortfunktion des Mailprogramms führte zur Zustellung der Mail an die modifizierte externe Mail-Adresse und zu dem Irrtum, dem Firmenleiter an dessen Firmen-E-Mailadresse zu schreiben.

Eine ausführliche Beschreibung des Modus Operandi finden Sie in einem Artikel der WirtschaftsWoche vom 18.08.2015 unter:
http://www.wiwo.de/erfolg/management/falsche-chefs-zocken-firmen-ab-den-enkeltrick-gibts-auch-bei-unternehmen/12201572.html

Folgende Hintergründe sollten Sie kennen:

Diese digitale Version des „Enkeltricks“ erlebt seit ca. zwei Jahren stetig steigende Erfolge verbunden mit hohen Schadenssummen.

Ein Schutz gegen diese Angriffsmethode ist das Hinterfragen der Identität des Kommunikationspartners über einen anderen Kommunikationsweg.

Sind die Legitimierungsdaten plausibel? Ist nicht nur der angezeigte Name, sondern auch die dahinterliegende E-Mail-Adresse stimmig.

Der Freigabeprozess solcher Überweisungen sollte immer nach dem Vieraugen-Prinzip von zwei unabhängig beteiligten Mitarbeitern begleitet werden.

Weitergehende Informationen zu den verschiedenen Angriffsarten und wie man sich schützen kann finden Sie im Internet auf der Seite des Verfassungsschutz Niedersachsen unter Wirtschaftsschutz / Newsletter:

http://www.verfassungsschutz.niedersachsen.de/portal/live.php?navigation_id=12301&article_id=54241&_psmand=30