Niedersächsisches Ministerium
für Inneres und Sport

Wirtschaftsschutz - *Info*

Hannover im Juli 2013

Sehr geehrten Damen und Herren,

Inventarisierung und Kontrolle der eingesetzten Hardware ist in Unternehmen eine ungeliebte Aufgabe, welche auch gerne mal unterbleibt.

Aus gegebenem Anlass möchten wir Ihnen einen aktuellen Fall zum Themenfeld Datenausspähung durch manipulierte Hardware näher bringen, der dem niedersächsischen Wirtschaftsschutz gemeldet wurde.

Es zeigt sich hier, wie wichtig es ist, auch im Bereich der eingesetzten Hardware in Unternehmen den Soll-Zustand zu kennen und diesen regelmäßig mit dem Ist zu vergleichen.

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

Ein mittelständisches Unternehmen aus dem produzierenden Gewerbe verliert in zunehmendem Maße Aufträge an den Wettbewerb. Dieses besonders bei Ausschreibungen, bei denen das Angebot per Email abgegeben wurde. Angebote die per FAX an den Auftraggeber übermittelt wurden, bekamen in der Regel den Zuschlag. Durch Zufall wurde in einer Produktionshalle ein WLAN-Router aufgefunden, welcher mit einem Steuerungscomputer verbunden war. Auf Nachfrage des Firmenleiters konnte niemand Sinn und Zweck des Gerätes erklären. Es war auch keinem Mitarbeiter bekannt, ob der Router Firmeneigentum war. In dieser Situation wurde der Wirtschaftsschutz um Hilfe und Unterstützung gebeten.
Die forensische Untersuchung des WLAN-Routers ergab, dass der Router auf die internen IP-Adressräume des Unternehmens eingestellt war. Als Besonderheit ist hier festzustellen, dass eine weitere IP-Adresse, die nicht mit dem Unternehmensnetzwerk kompatibel ist, eingetragen wurde. Offensichtlich hatten unbekannte Täter hier im Unternehmensnetzwerk ein für die Administratoren der Firma unsichtbares zweites Netzwerk eingerichtet. Es steht zu vermuten, dass hier ein Innentäter Informationen zu Angeboten abgeschöpft und an den Wettbewerb weitergegeben hat. Weitere Ermittlungen dauern noch an.

<u>Folgende Hintergründe sollten Sie kennen:</u>

Es ist nach wie vor geübte Praxis von professionellen Informationsbeschaffern, unter Zuhilfenahme von empfänglichen Mitarbeitern, IT-Hardware zum Zwecke der Datenausleitung zu manipulieren.

<u>Fazit:</u>

Deshalb ist eine regelmäßige Überprüfung der eingesetzten Hardware durch die zuständigen Fachbereiche anzuraten.