BVT

WIS[sen]

SCHUTZ DURCH WISSEN

WIRTSCHAFTS- UND INDUSTRIESPIONAGE

DAS BULLETIN

Ausgabe 1/2016

IN DIESER AUSGABE

CEO-Fraud bzw. Fake-President Trick

- Vorgehensweise und Erfolge
- Finanzieller Schaden oder Datenabfluss
- Schutzmaßnahmen

- **NEU!** - Studie „Wirtschafts- und Industriespionage in österreichischen Unternehmen 2015“

BM.I

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES

Impressum:
Medieninhaber: Bundesministerium für Inneres, Generaldirektion für die öffentliche Sicherheit, 1014 Wien, Herrengasse 7, Telefon: +43 (0)1-53126-0, E-Mail: einlaufstelle@bmi.gv.at, www.bmi.gv.at
Inhaltlich verantwortlich: Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (.BVT), 1014 Wien, Postfach 100, Herrengasse 7, Telefon: +43 (0)1-53126-4100, E-Mail: WIS@bvt.gv.at
Gestaltung: Bundesministerium für Inneres, Abteilung I/8 - Protokoll und Veranstaltungsmanagement

WKO WIRTSCHAFTSKAMMER ÖSTERREICH

TU WIEN TECHNISCHE UNIVERSITÄT WIEN Vienna University of Technology

iv INDUSTRIELLEN VEREINIGUNG

WIRTSCHAFTS- UND INDUSTRIESPIONAGE

Sehr geehrte Damen und Herren,

seit Beginn des Jahres 2015 konnten Kriminelle durch CEO-Fraud – ebenso als Fake-President Trick bekannt – bereits Millionen Euro erbeuten. Mit teils immensen finanziellen Verlusten für das betroffene Unternehmen und Folgen für die getäuschten Mitarbeiterinnen und Mitarbeiter.

Wie ein aktueller Fall eines oberösterreichischen international tätigen Industrieunternehmens zeigt, bedarf es keiner rein extern gesteuerten Hackerangriffe um Österreichs Unternehmen zu schädigen. Ein Unternehmen ist nur durch aufmerksame Mitarbeiter und Mitarbeiterinnen vor Wirtschafts- und Industriespionage, oder wie in diesem Fall, vor sogenannten CEO-Fraudsters sicher.

Es handelt sich um organisierte kriminelle Gruppen mit guten Kenntnissen über die Branchenstruktur, mitunter auch über bevorzugte externe Dienstleister, wie beispielsweise Steuerberater, Rechtsanwaltskanzleien, etc.. Ebenso nutzen die Täter Informationen die Unternehmen in öffentlich zugänglichen Medien, sei es die unternehmenseigene Homepage, in Werbebroschüren, auf Messen oder durch die Beteiligung an öffentlich geförderten Projekten bereitstellen.

Es gilt den Kontakt zu Mitarbeiterinnen oder Mitarbeitern im Unternehmen herzustellen, die über Zahlungsanweisungsbefugnisse oder den Zugang zu relevanten vertraulichen Informationen verfügen. Dies kann der CFO, ein befugter Sachbearbeiter oder ebenso ein Kundenbetreuer (Key Account Manager) sein. Sind die jeweiligen Ansprechstellen nicht via Internet in Erfahrung zu bringen, so genügt im Regelfall ein einfacher Anruf im Unternehmen, um die Kontaktdaten des späteren Opfers zu erlangen.

Der Fake-President Trick ist heruntergebrochen klassisches Social Engineering, dh. die Beeinflussung von Menschen zur unrechtmäßigen Generierung von Informationen bzw. Vorteilen. Das Verantwortungs-bewusstsein der, im Regelfall via E-Mail kontaktierten, Mitarbeiterin oder des Mitarbeiters, im Auftrag des Vorgesetzten ihrer bzw. seiner Arbeitsaufgabe nachzukommen, führt die Täter zum Erfolg.

Strotzten die E-Mails anfangs noch vor Fehlern, zumeist aufgrund der (schlechten) Übersetzungssoftware, werden diese in den letzten Monaten zusehends qualitativ hochwertiger und personalisierter.

Im Regelfall folgen der Inhalt der E-Mails sowie die weitere Kommunikation mit dem CEO Fraudster einem klaren Muster:

- Die Empfängerin oder der Empfänger der E-Mail wird darauf hingewiesen, dass es sich um einen sehr dringenden Auftrag (Zahlungsanweisung, Übermittlung von Dokumenten) handelt, und darüber jedenfalls Stillschweigen zu bewahren sei. Oftmals wird ein Geschäftsvorgang aus der Vergangenheit angeführt, welcher angeblich aufgrund mangelnder Verschwiegenheit der handelnden Personen nicht erfolgreich abgeschlossen werden konnte.
- Des Weiteren solle die Empfängerin oder der Empfänger jedenfalls direkt auf diese E-Mail antworten und keine neue Konversation starten. Bei einem prüfenden Blick auf die Reply-to-Adresse fällt der Betrugsversuch zumeist auf, denn diese ist nicht ident mit der tatsächlichen E-Mail Adresse des „Absenders“ bzw. CEOs. Vielmehr handelt es sich häufig um Adressen eines Freemail-Anbieters aus dem nicht-europäischen Ausland.
- Formulierungen in der E-Mail zielen auf die Verlässlichkeit und Vertrauenswürdigkeit der Mitarbeitern bzw. des Mitarbeiters ab, und bauen einen gewissen Druck auf, unmittelbar und ohne Rücksprache zu agieren, da der Erfolg des Geschäftsvorgangs von ihrem oder seinem Handeln abhängig ist.

SCHUTZMAßNAHMEN

Sensibilisieren Sie die Mitarbeiterinnen und Mitarbeiter aller etwaig betroffenen Unternehmensbereiche für diese Betrugsmethode!

Klare interne Prozesse und Vertretungs- bzw. Abwesenheitsregelungen führen zu Handlungssicherheit der agierenden Mitarbeiterinnen und Mitarbeiter.

Die direkte Rücksprache mit der vermeintlichen Absenderin oder dem Absender zur Verifizierung der Echtheit der E-Mail mittels interner Rufnummer oder einer E-Mail unter Verwendung des internen Adressbuches schaffen Klarheit.

Mitunter arbeiten CEO-Fraudster mit Mitteilungen hinsichtlich der Änderung von Bankverbindungen bestehender Lieferanten oder sonstiger Gläubiger. Hier sollte nach erfolgter unternehmensinterner Überprüfung ebenso mit dem Geschäftspartner direkt, über die bereits bekannten Kontaktmöglichkeiten, Rücksprache gehalten werden.

Es sollten grundsätzlich keine manuellen Geldanweisungen an bislang unbekannte (ausländische)

Bankverbindungen, insbesondere in Länder wohin keine Geschäftsbeziehungen bestehen getätigt werden. Eine IT-basierte Beschränkung kann das Risiko erheblich verringern.

Für die Übermittlung sensibler Geschäftsunterlagen sollten ebenfalls interne Genehmigungsprozesse etabliert werden.

Allgemein gilt: Achten Sie auf die öffentlich über Ihr Unternehmen verfügbaren Informationen!

Bei Verdachtsfällen und Fragen wenden Sie sich an die Sicherheitsbehörden!

Durch Meldungen von Verdachtsmomenten bzw. kritischer Situationen in Bezug auf Wirtschafts- und Industriespionage im In- oder Ausland ist es dem BVT als kompetentem und vertrauenswürdigem Ansprechpartner möglich, Risikoprofile zu erstellen und dadurch aktuelle Trends aufzuzeigen.

STUDIE „WIRTSCHAFTS– UND INDUSTRIESPIONAGE IN ÖSTERREICHISCHEN UNTERNEHMEN 2015““

Im Auftrag des Bundesministeriums für Inneres (Durchführung BVT – Präventionsprogramm WIS) und in enger Kooperation mit der Wirtschaftskammer Österreich und der Industriellenvereinigung wurde durch die FH Campus Wien eine Studie zur Betroffenheit der österreichischen Unternehmen von Wirtschafts- und Industriespionage erstellt. Die Studie wurde am 20. Jänner 2016 in den Räumlichkeiten des BM.I vor Vertreterinnen und Vertretern der Wirtschaft präsentiert.

BK-Direktor Lang, BVT-Direktor Gridling, IV-Vizegeneralsekretär Koren, FH-Professor Langer, Innenministerin Mikl-Leitner, Burger-Scheidlin (ICC), Generaldirektor Kogler, BVT-Abteilungsleiter Weiss (v.l.n.r.)

Foto: LPD Wien/Karl Schober

Die Ergebnisse zeigen, dass jedes österreichische Unternehmen von Wirtschafts- und Industriespionage betroffen sein kann. 5,1 Prozent der befragten Unternehmen gaben an, dass ihr Unternehmen in den vergangenen fünf Jahren mindestens einmal Opfer von Wirtschafts- und Industriespionage war. Dies entspricht hochgerechnet 8.400 Unternehmen. Ein Drittel der Vorfälle betraf Industriebetriebe. 22 Prozent der betroffenen Unternehmen waren von fünf oder mehr Vorfällen betroffen. Bei 71 Prozent der betroffenen Unternehmen entstanden erhebliche mittel- bis langfristige Schäden, etwa der Verlust von Aufträgen oder Kunden sowie die Schädigung des Unternehmensansehens. Der finanzielle Gesamtschaden beträgt jährlich etwa eine Milliarde Euro.

Die Studie ist unter

http://www.bmi.gv.at/cms/BMI_Verfassungsschutz/wis

abrufbar.

AUSBLICK

Welche Informationen liegen dem Unternehmen über eine aktive oder potentielle zukünftige Mitarbeiterin oder einen Mitarbeiter vor und wie sind diese zu bewerten? Die Sicherheitsüberprüfung gemäß §§ 55ff Sicherheitspolizeigesetz ist eine Möglichkeit zur Beantwortung der Frage nach der Vertrauenswürdigkeit von Personen und wird auf Antrag des Unternehmens durch das BM.I/BVT vorgenommen. Die Ausgabe 2/2016 behandelt dieses Thema und führt die Hintergründe, Voraussetzungen und Vorgehensweise im Zusammenhang mit Sicherheitsüberprüfungen an.

VERANSTALTUNGEN

- 03.03.2016 — WKÖ - E-Day:16 „Unternehmen Sicherheit“ Im Spannungsfeld von Mensch und Technik; 1045 Wien, Wiedner Hauptstraße 63.
- 11.-15.04.2016 — Lehrgang ManagerIn für Wirtschaftsschutz (WIS-M) - TU Wien und BVT; WIFI Dornbirn.

KONTAKT

Für weiterführende Informationen und im Anlassfall steht Ihnen das .BVT zur Verfügung:

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

E-Mail: wis@bvt.gv.at
Telefon: +43-(0)1-53126-4100

http://www.bmi.gv.at/cms/BMI_Verfassungsschutz/wis