BVT

WIS[sen]

SCHUTZ DURCH WISSEN

WIRTSCHAFTS- UND INDUSTRIESPIONAGE

DAS BULLETIN

AUSGABE 1/2015

IN DIESER AUSGABE

Social Engineering

- Vertrauen schaffen und Informationen gewinnen
- Unternehmenskultur als Schutzschild
- Informationen und Ausblick

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

FH CAMPUS WIEN UNIVERSITY OF APPLIED SCIENCES

iv INDUSTRIELLEN VEREINIGUNG

WIRTSCHAFTS- UND INDUSTRIESPIONAGE

Sehr geehrte Damen und Herren,

Im Umgang mit anderen Menschen schätzen wir Eigenschaften wie Hilfsbereitschaft, Flexibilität und Kompetenz. Mitarbeiterinnen und Mitarbeiter die sich mit ihrer Arbeit identifizieren gelten als motiviert und dies geht im Regelfall mit einer positiven Wirkung auf das Betriebsklima einher. Ein kurzer Smalltalk in der Gemeinschaftsküche, beim Getränkeautomaten oder Stockwerksdrucker – klassischen Kommunikationsinseln innerhalb eines Unternehmens – tragen dazu bei, Vertrauen zu anderen Mitarbeiterinnen und Mitarbeitern aufzubauen, Neuigkeiten aus anderen Fachabteilungen auszutauschen oder schlicht über die Wochenendplanung mit der Familie zu philosophieren.

So können kurze, unverbindliche Gespräche – Smalltalk – bei gegenseitiger Sympathie und beispielsweise über das Erkennen von Gemeinsamkeiten die Vorstufe für tiefergreifende Gespräche sein. Hierdurch wird Vertrauen aufgebaut. Dieses Vertrauen unter Mitarbeiterinnen und Mitarbeitern des Unternehmens bzw. unter Geschäftspartnern ist unerlässlich für die Bildung, Aufrechterhaltung und Weiterentwicklung von Geschäftsbeziehungen bzw. einer entsprechenden Unternehmenskultur, und somit für den Erfolg eines Unternehmens.

Mitarbeiterinnen und Mitarbeiter, als wichtigste Wissensressource eines Unternehmens, nehmen unterschiedliche Rollen in ihrem Berufs- und Privatleben ein und treten über soziale Netzwerke, sei es virtuell oder real – beispielsweise über Hobbys, in Interaktion mit anderen Menschen.

Social Engineering – im Zusammenhang mit Wirtschafts- und Industriespionage, meint die Beeinflussung von Menschen zur unrechtmäßigen Generierung von unternehmensinternen Informationen. Je mehr Informationen über eine Mitarbeiterin oder einem Mitarbeiter dem Angreifer, dem Social Engineer, vorliegen, umso leichter fällt es ihr oder ihm eine Vertrauensbasis zu dieser Mitarbeiterin oder diesem Mitarbeiter aufzubauen, um im Endeffekt an die gewünschten Informationen zu gelangen. Anknüpfungspunkte sind oftmals die eingangs erwähnten Eigenschaften, insbesondere die Hilfsbereitschaft, der Stolz der Mitarbeiterin oder des Mitarbeiters auf berufliche Erfolge oder das Gegenteil, die Unzufriedenheit mit der gegenwärtigen Arbeitssituation.

Die Beispiele hierfür sind sehr vielfältig, von der frustrierten Mitarbeiterin oder dem frustrierten Mitarbeiter, die oder der bei einem Feierabendbier über ihre bzw. seine Arbeit meckert, die hilfsbereite Mitarbeiterin oder der hilfsbereite Mitarbeiter, die oder der einen Besucher schnell an einen Computer lässt, um noch rasch eine dringend benötigte E-Mail auszudrucken, oder die Mitarbeitern die bzw. der Mitarbeiter der auf eine telefonische oder schriftliche Anfrage über unternehmensinterne Daten, dem „neuen externen Dienstleister“ diese übermittelt, da die Daten versehentlich in Verlust geraten sind.

DIE DREI ANGRIFFSTYPEN DES SOCIAL ENGINEERING

Angreifern fällt es oftmals leicht durch die Verwendung des Internets und insbesondere der sozialen Netzwerke an persönliche Informationen von Mitarbeiterinnen und Mitarbeitern zu gelangen. Diese Informationen wie beispielsweise Hobbys, die Position im Unternehmen bzw. der Aufgabenbereich oder schlicht das Lieblingslokal können für die klassische Form des „Human Based Social Engineerings“ genutzt werden. Die direkte Interaktion mit Menschen, ist trotz der technischen Möglichkeiten, die schnellste und effektivste Möglichkeit an gewünschte Informationen zu gelangen.

ANGRIFFSTYPEN

- Human Based Social Engineering
- Reverse Social Engineering
- Computer Based Social Engineering

„Reverse Social Engineering“ ist eine weitere Methode, bei welcher der Angreifer gezielt eine Situation herstellt, in der das Opfer selbst den Kontakt herstellen möchte. Dies geschieht beispielsweise durch die Verursachung eines Problems, dem sich die Betroffene oder der Betroffene (das Opfer) hilflos gegenüber sieht, und den Kontakt bzw. die Hilfe des Angreifers sucht.

Weniger spektakulär als die Verursachung eines technischen Gebrechens in den Unternehmensräumlichkeiten, um hierdurch getarnt als Techniker oder Sachverständiger Zutritt zu erlangen, geschieht Reverse Social Engineering jedoch in sozialen Netzwerken. Ziel ist ebenfalls, den Nutzer dazu zu bewegen, den Angreifer von sich aus zu kontaktieren.

Hier werden grundsätzlich drei Arten des Reverse Engineering unterschieden. So werden im Falle des vorschlagsbasierten Reverse Social Engineering durch die gezielte Nutzung der von sozialen Netzwerken verwendeten Algorithmen bestimmte Aktionen gesetzt, welche zur Folge haben, dass das Profil des Angreifers der Nutzerin oder dem Nutzer zB. als neue Freundin oder als neuer Freund vorgeschlagen wird. Demographiebasiertes Reverse Social Engineering orientiert sich an Ähnlichkeiten in den Profilen des Opfers und des Angreifers, um dadurch die Aufmerksamkeit und das Vertrauen des Opfers zu erlangen. Das zugriffsorientierte Reverse Social Engineering nutzt die „soziale Medien Eitelkeit" der Opfer aus, indem durch oftmaliges Zugreifen auf deren Profil, ihre oder seine Neugierde geweckt wird, und letzten Endes die Kontaktaufnahme wiederum durch das Opfer erfolgt.

Reverse Social Engineering in sozialen Netzwerken

- Vorschlagsbasiertes Reverse Social Engineering
- Demographiebasiertes Reverse Social Engineering
- Zugriffsorientiertes Reverse Social Engineering

Das „Computer Based Social Engineering" stellt den dritten Typ des Social Engineerings dar, kann jedoch in der Realität oftmals nicht klar gegenüber dem Human Based Social Engineering und dem Reverse Social Engineering in sozialen Netzwerken, abgegrenzt werden. Hier werden im Regelfall real existierende Webseiten kopiert, oder E-Mails mit „ansprechenden" Betreffzeilen oder Datenanhängen versendet, um diese mit Schadsoftware zu hinterlegen und hierdurch an Daten, zumeist Passwörter oder Zugriffsberechtigungen zu gelangen.

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

Unternehmenskultur als Schutzschild

All diesen Methoden des Social Engineering ist gemeinsam, dass ihre Anwendung im Unternehmen nicht durch strikte Verhaltens-Regeln für die Mitarbeiterinnen und Mitarbeiter, unterbunden werden kann. Wenngleich allgemeine Verhaltensregeln, wie z.B. das Sperren des Computerbildschirms und das Versperren des Büros zum Schutz vor dem Zugriff betriebsfremder Personen auf Unterlagen und das Computernetzwerk oder das verpflichtete Tragen des Firmenausweises für Mitarbeiterinnen und Mitarbeiter zur Unterscheidung von fremden Personen, bestimmte Angriffe erschweren, so bedarf es der Einbindung aller Mitarbeiterinnen und Mitarbeiter als „Schutzschild" gegen Wirtschafts- und Industriespionage.

Die Sensibilisierung bezüglich der von Angreifern angewandten Techniken und der potentiellen persönlichen Angriffspunkte, das Reflektieren des eigenen Agierens in Situationen sowie konkrete Ansprechpersonen innerhalb des Unternehmens im Verdachtsfall bieten die Grundlage für ein, vor Social Engineering Angriffen, geschütztes Unternehmen. Entscheidend ist die aktive Einbindung der Mitarbeiterinnen und Mitarbeiter sowie die Stärkung ihrer Handlungskompetenz.

So muss sich eine Mitarbeiterin oder ein Mitarbeiter sicher fühlen, die Unterstützung des Managements zu genießen, wenn sie oder er im Zweifelsfall, beispielsweise einem Auskunftsersuchen nicht unmittelbar nachkommt, um Rücksprache mit dem Management bzw. der oder dem Sicherheitsverantwortlichen zu halten. Das Bedürfnis nach Eingebundenheit und Zugehörigkeit zu einem Unternehmen kann durch Veranstaltungen welche ebenso einen Sensibilisierungs- sowie Schulungszweck beinhalten und nach dem „need to share-Prinzip" gestaltet sind, positiv beeinflusst werden, und unternehmensintern das gegenseitige Vertrauen stärken.

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

AUSBLICK

Die Bewertung interner Informationen als Geschäftsgeheimnisse sowie die Berechnung des monetären Schadens bei deren Verlust durch Wirtschafts- oder Industriespionage gestaltet sich oftmals sehr schwierig. Die Ausgabe 2/2015 enthält nützliche Informationen sowie Expertenmeinungen zu diesem Thema.

VERANSTALTUNGEN

- 05.03.2015 E-Day 2015 unter dem Motto „Mehr Spielraum für Unternehmen", WKÖ Wien
- 11.-13.03.2015 4. Wintertagung des BVSW und PROTECTOR unter dem Motto „Grenzen der Sicherheit", Arabella Alpenhotel am Spitzingsee
- 22.-23.04.2015 Security Forum, FH Oberösterreich Campus Hagenberg