Bundesministerium
Inneres

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Wirtschafts- und Industriespionage

Cybersicherheit

Leitfaden

WIS[sen]
SCHUTZ DURCH WISSEN
WIRTSCHAFTS- UND INDUSTRIESPIONAGE

Wirtschafts- und Industriespionage

Der Wirtschaftsstandort Österreich ist geprägt durch eine Unternehmenslandschaft, wobei insbesondere Klein- und Mittelbetriebe eine große Rolle spielen. Diese Klein- und Mittelbetriebe bilden das Rückgrat der österreichischen Wirtschaft. Diese gilt es zu schützen.

Aufgabe des BVT im Bereich Wirtschaftsschutz ist es, neben der operativen Fallbearbeitung von Wirtschaftsspionage aktiv in der Prävention aufzutreten.

Der Schutz eines Unternehmens vor Wirtschafts- und Industriespionage beschränkt sich nicht ausschließlich auf den Gebäudeschutz, die IT Sicherheit und die Schulung der Mitarbeiterinnen und Mitarbeiter über den Umgang mit Daten und Unterlagen.

Durch die fortscheitende Digitalisierung und der internationalen Vernetzung gewinnt die Präsentation von Unternehmungsprodukten weltweit an Bedeutung. Die Angriffsziele können daher vielfältig sein.

Was können Sie bzw. ihr Unternehmen dagegen tun.

Nach wie vor spielt der Faktor Mensch eine bedeutende Rolle. In 71,2% der Fälle ist der „Faktor Mensch“ in Tathandlungen involviert.

Als Auslöser oder Motivation für solche Tathandlungen können unter anderem fehlende berufliche Perspektive, berufliche Unzufriedenheit, materielle Vorteile, Geldgier, finanzielle Problem oder auch Liebesbeziehungen, Abenteuerlust, Geltungsbedürfnis und andere charakterliche oder psychologischen Aspekte sein.

Mitarbeiter als wichtigster Wissensträger

Ihre Mitarbeiter sind Ihr wichtigster Unternehmenswert. Aufgrund ihres Wissens sind sie für Spione ein vielversprechendes Angriffsziel.

Tipps

- Informieren und sensibilisieren Sie sich und Ihre Mitarbeiter
- Achten Sie auf die Motivation, Zufriedenheit und private Notlagen Ihrer Kollegen.
- Stellen Sie unternehmensinterne Regeln im Umgang mit Daten und Dritten auf und leben sie diese vor!
- Fördern sie eine Unternehmenskultur des guten Miteinanders.

Social Engineering

Social Engineering ist die Methode, die Ihre Mitarbeiter meist über zwischenmenschliche Beziehungen manipuliert und sie zur Preisgabe von Know-how bewegen kann. Ausgenutzt werden daher menschliche Eigenschaften wie beispielsweise Vertrauen, Eitelkeit, Hilfsbereitschaft, Habgier, Angst oder Respekt vor Autoritäten.

Sie wird z.B. auf Messen, Veranstaltungen, in sozialen Medien oder über fingierte E-Mails, inszenierte Forschungsangebote oder Headhunter Kontakte eingesetzt.

Frustration am Arbeitsplatz

Ein schlechtes Arbeitsklima oder persönliche Notlagen machen Mitarbeiter zu einem leichten Angriffsziel. Sie können dadurch zu Innentäter werden.

„Zufriedene Mitarbeiter sind loyal und damit die wichtigste Sicherheitsmaßnahme.“

50% Innentäter

50% Außentäter

Vorsicht bei Reisen

Besonders auf Auslandsreisen sind Mitarbeiter gefährdet, Opfer von ausspähung zu werden. In einigen Ländern erlaubt die Rechtslage den gezeilten Zugriff auf Ihre Daten, z.B. bei Einreisekontrollen Kommunikation Internetnutzung und durch Verschlüsselungsverbote.

Denken Sie daran, dass Ihre Mitarbeiter neben Ausspähung auch Opfer von Kidnapping, Erpressung, Diebstahl, oder anderen kriminellen Handlungen in Ländern mit fragiler Sicherheitslage werden können.

- Informieren sie sich schon vorab über die Sicherheits- und Rechtslage vor Ort.
- Verwenden sie nach Möglichkeit ein spezielles Reiseequipment z.B. Reise Laptop, Handy usw.
- Nehmen sie kritische Daten nur ausrechend verschlüsselt oder gar nicht mit.
- Seien sie sich bewusst: im öffentlichen Raum kann jeder mithören und mitlesen.
- Schützen sie ihren Laptop mit Sichtschutzfolie.
- Nutzen sie kein öffentliches WLAN ohne zusätzlichen Schutz.

Sollte Ihnen so etwas passieren, verständigen sie das BVT.

Innovationen geheim halten

Innovationen sichern Markterfolg und Wettbewerbsvorsprung Ihres Unternehmens. Dies kann sich schnell ändern, wenn es Ihnen nicht gelingt, Ihre Entwicklungsstandorte und Ihr Know- how ausreichend zu schützen.

- Forschungs- und Entwicklungsbereiche nie frei zugänglich machen.
- Schließen sie Geheimhaltungsverträge mit Dienstleister ab.
- Lassen Sie Besuchergruppen nicht unbeaufsichtigt.

Sicherheit der Geschäftsleitung

- Entwickeln sie ein Sicherheitskonzept für ihr Unternehmen
- Seien Sie Vorbild bei der Einhaltung der Sicherheitsregeln
- Achten Sie in Gesprächen mit Partner, Dritten und in sozialen Netzwerken darauf, was Sie preisgeben.

Schwachstelle Maschine

Sabotage

- Ihr Unternehmen kann durch die mutwillige Beschädigung Ihrer Produktionsprozesse, Betriebsabläufe oder Produkte große Schäden erleiden und die Konkurrenzfähigkeit verlieren.
- Durch die Digitalisierung werden Produktionsanlagen und moderne Informations-und Kommunikationstechnik vernetzt. Dadurch entstehen wechselseitige neue Gefährdungen.
- Täter versuchen, Know-how über Produktionsprozesse zu gewinnen, um sich dadurch einen Wettbewerbsvorteil zu verschaffen.

Einkauf, Zulieferer und Dienstleister

- Binden sie Dienstleister und Zulieferer in Ihr Schutzkonzept ein.
- Regeln sie den Umgang mit vertraulichen Daten
- Daten über Dienstleister sind sensible Informationen, die genauso schützenswert sind wie ihr eigenes Know-how.
- Stellen sie sicher, dass Ihre Unternehmensdaten bei Outsourcing nicht missbraucht werden können.

INNENTÄTER

…ein unterschätztes Risiko für Unternehmungen.

Beachten Sie Täter können ALLE sein vom Hausmeister bis zum Manager

Cybersicherheit

Lage, Trends und Erfahrungsaustausch

Dipl.-Ing. Philipp BLAUENSTEINER
Leitung Cyber Security Center
Wien, 14.05.2019

Das verbreitete Klischee, wonach es sich bei Cyberkriminellen zumeist um männliche, jugendliche Einzeltäter mit extrem hohem IT-Knowhow handelt, entspricht nicht mehr der Realität. Die Bandbreite möglicher Täter bzw. Tätergruppen ist heute wesentlich breiter als früher. Zu den häufigsten Tätergruppen gehören **Kriminelle**, **Hacktivisten**, **staatliche Akteure**, **Experten auf Abwegen**, **Insider** oder auch **Script Kiddies**. Die Motivation kann Sabotage, Spionage, Frustration, (Hacker-)Sport oder zumeist schlicht Geld sein.

Der Bericht Cybersicherheit 2019 (derzeit noch nicht publiziert) zeigt als mit Abstand häufigste Form der Cyberkriminalität in Österreich **Angriffe durch Ransomware (Cryptolocker)**, gefolgt von Phishing-Angriffen (einschließlich CEO-Fraud) und zielgerichteten Angriffen auf Basis von APTs (Advanced Persistent Threats). Die Studie Cyber Security in Österreich 2019 (KPMG) zeigt dabei anschaulich, dass **Cybersicherheit zu einer zentralen Herausforderung für Unternehmen** wird. So sahen sich insgesamt 66 % der Unternehmen in Österreich im letzten Jahr mit einem Cyberangriff konfrontiert.

Derzeit steht vor allem die Bewältigung der folgenden Cyberangriffsarten im Fokus:

Ransomware

Als Ransomware werden Schadprogramme bezeichnet, die speziell dafür entwickelt wurden, den **Zugriff auf Daten und Computersysteme einzuschränken bzw. zu verhindern**. Sobald ein System mit der Schadsoftware infiziert ist, werden alle erreichbaren Daten verschlüsselt, sodass von den rechtmäßigen Nutzern nicht mehr darauf zugegriffen werden kann. Eine Wiederherstellung der Daten ist nur dann möglich, wenn nicht innerhalb einer bestimmten Zeit ein Lösegeld (engl. Ransom) an den Angreifer bezahlt wird.

Insbesondere im Zusammenhang mit Ransomware ist die **zeitgerechte und regelmäßige Durchführung von Datenbackups**, sowie die regelmäßige Überprüfung der ordnungsgemäßen Funktion, von essenzieller Bedeutung. Europol, sowie mehrere Strafverfolgungsbehörden der Europäischen Union betreiben gemeinsam mit großen Antiviren-Software-Unternehmen die **Plattform No More Ransom (https://www.nomoreransom.org)**. Ziel der Initiative ist, Opfern von Ransomware zu helfen.

CEO-Fraud

CEO-Fraud ist eine spezielle Angriffsart aus dem Bereich des Social Engineering. Sie nutzt vor allem **fehlende oder schlecht implementierte Sicherheitsprozesse in Organisationen oder Unternehmen**. Normalerweise geht einem CEO-Fraud-Angriff umfangreiche Aufklärungsarbeit des Angreifers in der Zielorganisation voraus. Je besser dem Angreifer Abläufe, Prozesse und handelnde Personen bekannt sind, desto höher sind seine Erfolgschancen.

Der eigentliche Angriff beginnt zumeist mit einer **gefälschten E-Mail an einzelne Mitarbeiterinnen oder Mitarbeiter der Finanzabteilung**, die vermeintlich vom Geschäftsführer des Unternehmens stammt. Darin wird ein, aufgrund der Aufklärungstätigkeit zumeist sehr plausibles Szenario gezeichnet, das stets darauf hinausläuft, dass der Geschäftsführer dringend für ein unvorhergesehenes, streng

vertrauliches Projekt (z.B. Anbahnung einer Firmenübernahme während einer Geschäftsreise) einen hohen Geldbetrag benötigt, den der Mitarbeiter sofort an ein bestimmtes Konto überweisen muss. Häufige Merkmale solcher Nachrichten sind unter anderem übertrieben große **Dringlichkeit**, enorme **Wichtigkeit** für Unternehmen, Hinweis auf eine **persönliche Verantwortung** des betroffenen Mitarbeiters, Verlangen nach unbedingter **Geheimhaltung**, betonte **Einschränkung der Kommunikationswege** oder gleich die **Untersagung jeglicher Rückfragemöglichkeit**.

Zur Vermeidung von CEO-Fraud ist eine entsprechende **Bewusstseinsbildung bei den verantwortlichen Mitarbeiterinnen und Mitarbeitern**, sowie die Implementierung von ausnahmslosen (!) Sicherheitsprozessen von entscheidender Bedeutung.

Advanced Persistant Threats (APTs)

Unter Advanced Persistent Threats (APTs) versteht man **zielgerichtete, fortschrittliche Angriffe** („advanced“), deren Vorbereitung und Durchführung mit extrem hohem personellen und finanziellen Aufwand durchgeführt wird. Diese Aufwände erreichen oftmals eine Größenordnung, die nahelegt, dass hinter der Entwicklung und Durchführung staatliche oder zumindest staatlich finanzierte Akteure stehen müssen. Dementsprechend stehen hinter einem APT-Angriff oft Motive wie Spionage oder Sabotage im großen Stil.

APTs sind so konzipiert, dass sie nach einer erfolgreichen Infektion des Zielsystems bzw. Zielnetzwerks **möglichst lange unentdeckt bleiben** („persistent“) und ihre Schadfunktion im Geheimen ausführen. Aufgrund der hohen Komplexität der Schadsoftware ist es sehr schwer (und oft auch nahezu unmöglich), das Vorhandensein eines APTs im eigenen Netz festzustellen. Dies stellt eine sehr große Bedrohung für das Opfer dar („threat“). Die **Erstinfektion erfolgt bei dieser Angriffsart sehr oft über klassisches Spearphishing**.