Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun Svizra

Nachrichtendienst des Bundes NDB

Wirtschaftsspionage

Wieso ein Film über Wirtschaftsspionage?

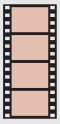
„Im Visier“ ist Teil des seit 2004 bestehenden Präventions- und Sensibilisierungsprogramms Prophylax des Nachrichtendiensts des Bundes (NDB). Der Kurzfilm wurde zu Ausbildungszwecken produziert mit dem Ziel, den Unternehmen und Institutionen Informationen über Wirtschaftsspionage zu vermitteln.

Die im Film gezeigte Vorgehensweise des ausländischen Nachrichtendiensts, um an vertrauliche oder geheime Informationen zu kommen, ist typisch für eine im Sinn ausländischer Nachrichtendienste oder privater Akteure zielführende Methodik, auch wenn die Ansatzpunkte im Detail variieren mögen. Die nachfolgenden Erläuterungen sollen das Verständnis des Publikums für die Feinheiten solcher Spionageaktionen erhöhen. Dabei werden weiterführende Informationen zu Vorgehensweisen und Spionagemethoden vermittelt sowie mögliche Schutzmassnahmen aufgezeigt, die ergriffen werden können, um das Spionagerisiko zu minimieren.

Vom Targeting zur Rekrutierung: Die Phasen eines Rekrutierungsversuchs

Die nachfolgend erläuterten Phasen sind nicht strikt voneinander trennbar, sondern können sich überlappen. Sie sind abhängig vom Ziel der Operation und von der Zielperson, von den eingesetzten Mitteln und der zur Verfügung stehenden Zeit sowie vom operativen Umfeld. Bestimmte Phasen können sehr kurz sein, während andere mehr Zeit in Anspruch nehmen. Zwischen dem Targeting und der Rekrutierung einer Zielperson liegen je nach Fall zwischen einigen Wochen und mehreren Monaten, in bestimmten Fällen sogar mehrere Jahre.

Targeting: Suche nach der geeigneten Zielperson und Abklärung von Angriffsflächen



OSINT und verdeckte Informationsbeschaffung

Mittels Online-Recherchen und der Konsultation öffentlicher Firmenprospekte der Grinder AG identifiziert der ausländische Nachrichtendienstoffizier, Frank Salov, den Leiter der Abteilung Forschung und Entwicklung, Stefan Jeger, als vielversprechende Zielperson. Jeger ist in verschiedenen sozialen Netzwerken mit einem umfangreichen Profil vertreten, wo er auch auf seine schriftstellerische Tätigkeit sowie seine nächsten Lesungen hinweist. Mittels verdeckten Observationen von Jeger sammelt Salov Bildmaterial und Erkenntnisse zu seinem Umfeld und seinen üblichen Aufenthaltsorten. Diese Informationen erlauben es Salov, Jegers Angriffsflächen und Schwachstellen zu sondieren.

Der Täter sucht Hinweise, die zu einer lohnenswerten Zielperson führen können, die die gesuchten Informationen liefern oder den Zugang zu diesen Informationen ermöglichen kann. Die Beschaffung von Informationen und Daten über die Zielperson kann mittels offener oder verdeckter Informationssammlung erfolgen:

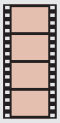
- **Open Source Intelligence (Osint)** ist die legale Beschaffung und Auswertung von Informationen aus öffentlich-zugänglichen Quellen wie Webseiten, Zeitungen und Zeitschriften, dem Besuch von öffentlichen Messen und Veranstaltungen, kostenlosen oder -pflichtigen Datenbanken, sozialen Medien usw. Insbesondere soziale Netzwerke (Facebook, Linkedin usw.) bieten oft eine Fülle von Informationen zu einer Person. Beruf, Fotos, Verbindungen, Hobbies, Beiträge in Online-Foren, Reisen usw. erlauben es, ein Profil der Zielperson mit ihren Gewohnheiten, Interessen, Kontakten, Leidenschaften und Frustrationen zu zeichnen.

- Bei der **verdeckten Informationsbeschaffung** werden nachrichtendienstliche Mittel eingesetzt, z. B. technische Überwachung oder physische Observation der Zielperson. Hier geht es u. a. darum, das Bewegungsmuster sowie weitere persönliche Kontakte und Aktivitäten der Zielperson zu erkennen.

Mögliche Schutzmassnahmen:

Wer Informationen (Dokumente, Bilder, Kommentare usw.) publiziert, hat es in der Hand, wie detailliert und tiefgründig sie oder er über sich selbst oder über ein Projekt, ein Produkt, eine Institution oder eine Firma und ihre Mitarbeiter und Mitarbeiterinnen informiert.

Anbahnung: Aufnahme des Kontakts zur Zielperson

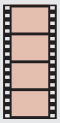


Der Erstkontakt

Salov nutzt die Tatsache, dass Jeger gerne schreibt und danach strebt, gelesen zu werden und seine Texte zu veröffentlichen. Er gibt sich als Literaturagent aus, um die Neugier und das Vertrauen Jegers zu wecken und den weiteren Kontaktaufbau zu erleichtern.

Der Erstkontakt mit der Zielperson wird minutiös vorbereitet. Hierfür dienen dem Nachrichtendienstoffizier oder dem privaten Akteur die in der Targetingphase gewonnenen Erkenntnisse zu den Gewohnheiten und den Schwachstellen der Zielperson. Diese Informationen ermöglichen es dem Täter, die richtige Ansprechbasis zu finden, ohne dass die Zielperson Verdacht auf illegitime Absichten hegt. Dabei nimmt der Nachrichtendienstoffizier oder der private Akteur oft eine entsprechende Tarnidentität an.

Kultivierung: Aufbau eines Vertrauens- und Abhängigkeitsverhältnisses



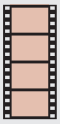
Ausnutzen der Schwachstelle als Hebel, Motivation oder Anreiz

Salov nutzt Jegers Leidenschaft fürs Schreiben gezielt aus. Im Literaturkaffee lobt er seine Lesung und täuscht gemeinsame Interessen vor. Als Salov Jeger in Aussicht stellt, im Literaturmagazin „Europe“ zu publizieren, sieht Jeger die Chance auf die Verwirklichung seines Lebenstraums gekommen. Dadurch schafft Salov ein Abhängigkeitsverhältnis: Jeger ist auf Salovs Hilfe angewiesen, wodurch er sich ihm gegenüber verpflichtet fühlt. Dieses Abhängigkeitsverhältnis wird weiter gefestigt, als sich Salov im Restaurant „Seesicht“ Jeger als Literaturagent zur Verfügung stellt.

Wird die Zielperson als potenziell geeignete Quelle eingestuft und ist das Eis gebrochen, wird eine Vertrauensbasis aufgebaut. Dazu instrumentalisiert der Täter „gemeinsame“ Interessen oder Leidenschaften. Er nutzt Schwachstellen der Zielperson gezielt als Hebel aus. Dieser Hebel kann die Form von Gefälligkeiten annehmen (z. B. dem Ego schmeichelnde Geschenke oder das Inaussichtstellen einer neuen Arbeitsstelle). Der nachrichtendienstlichtätige Akteur kann aber auch versuchen, sich kompromittierendes Material (Kompromat: Druck-/Erpressungsmittel) über die Zielperson zu beschaffen (Video- oder Bildaufnahmen, die die Zielperson z. B. beim Drogenkonsum, bei sexuellen Eskapaden oder bei der Annahme von Geld zeigen). Durch diese Kultivierung bildet sich eine Abhängigkeit der Zielperson gegenüber dem Täter und die Zielperson wird zunehmend erpressbar.

Abschöpfung

Gesprächsabschöpfung



Geschickte Gesprächsführung

Salov entlockt Jeger geschickt vertrauliche Informationen über seine Tätigkeit und die Forschungsprojekte der Grinder AG.

- Salov lädt Jeger ins gehobene Restaurant „Seesicht“ ein, um ihm vorzutäuschen, dass er Potenzial in ihm sieht, ihn wertschätzt und über bedeutende Mittel bzw. bedeutenden Einfluss verfügt.
- Salov lobt Jegers Textentwurf für das „Europe“. Er motiviert ihn, weiterzuschreiben.
- Als Jeger Salov erzählt, dass er Rundschleifmaschinen entwickelt, täuscht Salov Unwissen vor, damit ihm Jeger mehr darüber erzählt.

Sobald der Täter seine Zielperson in eine positiv (Anreize) oder negativ geprägte (Kompromat) Abhängigkeit gebracht hat, beginnt die Abschöpfung der gesuchten Informationen. Mit einer geschickten und subtilen Gesprächsführung entlockt er der Zielperson vermehrt sensible Informationen, ohne dass diese den Verdacht schöpft, dass sie dabei bedeutsame Hinweise liefert.

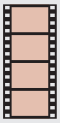
Mögliche Schutzmassnahmen:

Es ist wichtig zu wissen, welche Informationen schützenswert sind und nicht mit Dritten geteilt oder an diese weitergegeben werden dürfen. Das sind insbesondere jene Daten, deren Veröffentlichung oder Bekanntgabe dem Unternehmen oder der Institution Schaden zufügen kann. Fragt eine Person nach solchen bestimmten Informationen, so ist ein gewisses Misstrauen angebracht.

IT-/Cyberspionage

Die fortschreitende Digitalisierung und Vernetzung der Wirtschaft und Gesellschaft erhöhen die Anfälligkeit von Unternehmen, Institutionen und Privatpersonen für Cyberangriffe. Dem Schutz von elektronischen Daten und Kommunikationsnetzwerken bzw. -mitteln kommt daher eine zentrale Bedeutung zu. Doch nach wie vor stellt das Verhalten des Einzelnen den grössten Risikofaktor dar.

Social Engineering (soziale Manipulation)



Spear Phishing

Salov schickt Jeger einen Link, um den elektronischen Lebenslauf für Monsieur Simon, den Verleger des Literaturmagazins "Europe", auszufüllen. Durch das Anklicken des Links installiert Jeger unwissentlich auf seinem Firmencomputer eine Schadsoftware mit der Salov Zugriff auf das Firmennetz der Grinder AG erhält. Die Firma führt aber zwei getrennte Netzwerke: sensible Daten zu Forschungsprojekten und Technologien sind auf einem separaten Netzwerk abgelegt, das nicht mit dem Internet verbunden ist. Dadurch bleibt Salov der Zugriff auf diese Daten verwehrt.

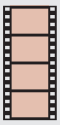
Social Engineering ist die psychische Beeinflussung von Personen mit dem Ziel, sie zur Preisgabe vertraulicher Daten oder zu bestimmten Aktionen zu bewegen. Im Bereich der Informationssicherheit wird Social Engineering oft dazu verwendet, um an Benutzernamen und Passwörter zu kommen sowie dazu, Viren und Trojaner zu verbreiten. Mitarbeiterinnen oder Mitarbeiter eines Unternehmens werden über soziale Medien, fingierte E-Mails oder Jobangebote angesprochen. Diese Angriffe können mittels Phishing bzw. Spear

Mögliche Schutzmassnahmen:

- Nur so viele Informationen wie nötig publizieren. Dies gilt insbesondere für die Publikation von Namen, Funktionen und Fotos von Mitarbeiterinnen und Mitarbeitern.
- Misstrauen gegenüber E-Mails mit unbekanntem Absender, insbesondere wenn diese einen Link oder einen Anhang enthalten.
- Sicherheitsvorschriften und eine unternehmensweite Sicherheitskultur, die alle Mitarbeiterinnen und Mitarbeiter miteinbezieht.

Phishing erfolgen: Während Phishing-Mails massenhaft an beliebige E-Mail-Adressen versandt werden, sind Spear Phishing-Mails auf die Mitarbeiterin oder den Mitarbeiter abgestimmt, die oder der angegriffen wird.

Smartphone



Infizierung eines Smartphones

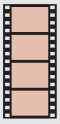
Im Restaurant „Seesicht" beobachtet Salov, wie Jeger auf seinem Smartphone seinen Zugriffscode eingibt. Mittels eines Ablenkungsmanövers verschafft sich Salov Zugang zu Jegers Smartphone und installiert eine Schadsoftware, die ihm den vollen Zugriff und die Kontrolle sämtlicher Funktionen ermöglicht. Er kann u. a. das Mikrofon anzapfen, wodurch er alle Gespräche von Jeger mit seinem Forschungsteam mithören kann.

Die in Smartphones vorhandenen Sensoren und Funktionen (GPS, Mikrofon, Kamera, heruntergeladene Applikationen, Adressbuch, WiFi, Bluetooth usw.) übermitteln sehr oft Daten bzw. Metadaten über die Benutzung des Smartphones oder den Benutzer. Die Auswertung dieser Daten durch Dritte ist daher ein einfaches Unterfangen. Eine Infizierung des Smartphones benötigt nicht unbedingt einen physischen Zugriff auf das Gerät; es existieren auch Methoden, die eine Infizierung aus der Ferne erlauben.

Mögliche Schutzmassnahmen:

- Elektronische Geräte verschlüsseln und nicht unbeaufsichtigt liegen lassen.
- Nur jene elektronischen Geräte und Dokumente auf Dienstreisen ins Ausland mitnehmen, die unbedingt benötigt werden.
- Vertrauliche Gespräche nie am Mobiltelefon tätigen.
- Vorsicht bei der Installation von Apps aus unbekannten Quellen.

USB-Stick



Infizierung elektronischer Geräte oder Datendiebstahl mittels USB-Stick

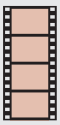
Linda setzt einen USB-Stick am Laptop des CEO der Grinder AG ein.

Der Einsatz von USB-Sticks ist ein weiteres Mittel, womit Computer und andere elektronische Geräte infiziert oder die darauf gespeicherten Daten durch Unbefugte heruntergeladen werden können. Eine Infizierung durch eine Schadsoftware (Virus, Trojaner usw.) mittels USB-Stick kann innert weniger Sekunden ausgeführt werden.

Mögliche Schutzmassnahmen:

Fremde oder geschenkt externe Peripheriegeräte (USB-Sticks, Computermäuse, externe Festplatten usw.) nicht benutzen. Solche Werbegeschenke können mit einer Schadsoftware infiziert sein.

Honeypot (Honigtopf)



Verführung

Nachdem die Versuche des ausländischen Nachrichtendiensts gescheitert sind, über Jeger an die gesuchten geheimen Informationen zu kommen, verführt Linda den CEO der Grinder AG, um sich Zugang zu dessen Laptop zu verschaffen.

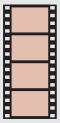
Als klassische Spionagetechnik bezeichnet der Begriff „Honeypot" den Versuch, eine Zielperson mittels sexueller Verführung abzuschöpfen bzw. zu rekrutieren. Entweder gibt die Zielperson die gewünschten Informationen von sich aus preis oder sie wird mittels Kompromat dazu erpresst.

(Der Begriff „Honeypot" wird auch im Cyberbereich verwendet und bezeichnet ein Computerprogramm oder einen Server, der die Netzwerkdienste eines anderen Rechners simuliert, mit dem Ziel, Informationen über einen möglichen Angreifer und dessen Angriffsmuster zu erhalten, ohne dabei das zu schützende Netzwerk zu gefährden.)

Mögliche Schutzmassnahmen:

- Persönliches Verhalten: darauf achten, was wem erzählt wird.
- Sicherheitsregeln des Unternehmens oder der Institution einhalten.
- Schutz der elektronischen Geräte vor unbefugten Zugriffen.

Rekrutierung(sversuch)



Abwendung eines Rekrutierungsversuchs

Jeger hat die Spionage durch den ausländischen Nachrichtendienst rechtzeitig bemerkt. Doch das Ziel von Frank Salov und Linda, an die geheime Technologie der Grinder AG zu kommen, bleibt bestehen. Mit der Verführung des CEO der Grinder AG durch Linda geht die Wirtschaftsspionage gegen das Unternehmen in die nächste Runde.

Einen Schritt weiter geht der Versuch, die Zielperson auf längere Zeit für die nachrichtendienstliche Mitarbeit, d. h. zur Beschaffung von vertraulichen bzw. geheimen Informationen zuhanden des ausländischen Nachrichtendiensts oder des privaten Akteurs, zu gewinnen. In den meisten Fällen sollte der Zielperson spätestens jetzt klar sein, dass ein staatlicher Nachrichtendienst oder ein privater Akteur im Spiel ist. Zeigt sich die Zielperson nicht kooperativ, versucht der Täter, erneut ihre Schwachstellen auszunutzen (v. a. durch Anwendung von Druckmitteln), oder er zieht sich zurück.

? … und im echten Fall eines erkannten Spionage- oder Rekrutierungsversuchs

Wird ein Spionageversuch gegen ein Unternehmen, eine Institution oder einen selbst bzw. ein Rekrutierungsversuch festgestellt, so ist es wichtig, dass umgehend die zuständigen Sicherheitsstellen im Betrieb und von diesen die Behörden (NDB oder Kantonspolizei) informiert werden. Der NDB sammelt Hinweise und wertet diese aus, wobei er für eine diskrete Behandlung und Bearbeitung des Spionagefalls sorgt. So können weitere Datenabflüsse und Schäden verhindert werden. Die Erkenntnisse über den Spionagefall und das Vorgehen der Täter tragen dazu bei, dass weitere Unternehmen und Institutionen besser geschützt und rechtzeitig auf mögliche Spionageversuche aufmerksam gemacht werden können. Dies erlaubt dem NDB, seine Präventionsmassnahmen an die aktuelle Bedrohungslage anzupassen.

Redaktion

Nachrichtendienst des Bundes NDB

Redaktionsschluss

Juni 2016

Kontaktadresse

Nachrichtendienst des Bundes NDB
Papiermühlestrasse 20
CH-3003 Bern
E-Mail: info@ndb.admin.ch

Video „Im Visier“

www.ndb.admin.ch