Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Nachrichtendienst des Bundes NDB

Merkblatt Wirtschaftsspionage

Einleitung

Beim strafgesetzlich verbotenen Nachrichtendienst (Spionage) geht es um die Beschaffung von bewusst vertraulich oder geheim gehaltenen politischen, wirtschaftlichen, militärischen, wissenschaftlichen oder technologischen Informationen oder Daten, sofern dies zum Nachteil der Schweiz oder ihrer Unternehmen, Institutionen oder von Personen in der Schweiz geschieht und die Informationen an einen ausländischen Akteur (Staat, Gruppierung, Unternehmen, Person usw.) weitergegeben werden.

Wie bedroht Spionage Ihr Unternehmen? Wie erkennen Sie Spionage und wie können Sie Ihr Unternehmen schützen? Einen vollständigen Schutz gibt es nicht; das Spionagerisiko lässt sich aber mit angemessenen Massnahmen verringern. Die folgenden Aufzählungen sind nicht abschliessend.

Wieso wird ein Unternehmen zum Ziel von Spionage?

- Das Unternehmen stellt Güter im Hochtechnologiebereich her und besitzt kritisches Know-how.
- Es bedient weltweit führend einen Nischenmarkt (Hidden Champion).
- Seine Güter unterliegen Exportkontrollen.
- Es betreibt angewandte Forschung und Entwicklung.
- Es hat Geschäftsbeziehungen zu Risikostaaten.

Welche Konsequenzen hat Spionage für ein betroffenes Unternehmen?

- Verlust von Geschäftsgeheimnissen
- Verlust von Aufträgen
- Verlust von Kunden
- Reputationsschaden – je nachdem auch für die Schweiz
- Personalentlassungen und finanzielle Einbussen bis hin zum Konkurs

Woher kommt die Spionagebedrohung?

- Besuche ausländischer Delegationen
- Joint Ventures, gemeinsame Forschungsprojekte, ausländische Investitionsabsichten, Beteiligungen an oder Erwerb von Unternehmen zwecks Technologietransfer
- Mitarbeiterinnen und Mitarbeiter, die unerlaubt vertrauliche Geschäftsinformationen oder -daten an Dritte weiterleiten, sei es aus Vorsatz oder Zwang (sog. Innentäter) oder aus Unachtsamkeit
- Social Engineering: u. a. (Spear-)Phishing-Angriffe[1], Kontaktaufnahme über soziale Netzwerke oder Telefon, gefälschte E-Mails im Namen eines Vorgesetzten (CEO-Betrug/CEO Fraud)
- Externe Dienstleister und Berater, Zulieferer
- Messen, Konferenzen
- Cyberangriffe

[1] Im Gegensatz zu Phishing-Mails, die breit gestreut werden, ist ein Spearphishing-Mail (oder eine Spearphishing-SMS) gezielt an einzelne Personen oder Gruppen innerhalb eines Unternehmens oder einer Organisation gerichtet und entsprechend formuliert. Die Zielperson wird aufgefordert, persönliche Informationen (z. B. Login-Informationen und Passwörter, sog. Credential-Phishing) preiszugeben oder einen Anhang zu öffnen bzw. auf einen Link zu klicken, der Schadsoftware enthält und den Computer der Zielperson und somit das Firmennetzwerk infiziert.

Schutzmassnahmen

- Erstellung und Umsetzung eines Informationssicherheitskonzepts und Ernennung einer dafür verantwortlichen Person, die mit Unterstützung der Geschäftsleitung die Sicherheitsmassnahmen durchsetzt
- Systematische und zentralisierte Kontrolle der vom Unternehmen und von seinen Mitarbeiterinnen und Mitarbeitern (inkl. Direktionsstufe) publizierten Informationen; Festlegen, was unter dem Gesichtspunkt des Informationsschutzes nicht veröffentlicht werden sollte
- Zutrittskontrollen und ständige Begleitung von externen Besuchern und Delegationen
- Segmentierung der IT-Netzwerke (z. B. Netzwerk der Forschungsabteilung vom restlichen Firmennetzwerk trennen und nicht mit dem Internet verbinden)
- Regelung und Einschränkung der Zugriffsrechte der Mitarbeiterinnen und Mitarbeiter auf Daten, Akten und Produkte, namentlich Forschungsergebnisse und Prototypen („Need to know"-Prinzip)
- Kein Anschluss von privaten USB-Sticks, Mobiltelefonen, Notebooks usw. an das Firmennetzwerk
- Verwendung von Zwei-Faktor-Authentifizierung für Zugänge zu Computern, Notebooks und E-Mails
- Regelmässige Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für Themen der Informationssicherheit und der IT-Sicherheit
- Keine vertraulichen Gespräche an öffentlichen Orten wie Restaurants, im Zug oder auch im Hotelzimmer, im Taxi oder am Telefon sowie keine Mitnahme von Mobiltelefonen zu Geschäftssitzungen, in denen sensitive Themen besprochen werden

Geschäftsreisen im Ausland

- Nur diejenigen elektronischen Geräte mitnehmen, die absolut nötig sind, diese verschlüsseln und die Geräte nie unbeaufsichtigt liegen lassen (gilt auch für Papierdokumente)
- Verwendung eines Notebooks, das nur für Auslandsreisen verwendet wird und keine sensiblen Daten enthält (sog. Reisenotebook), geschützt mit Firewall und Antivirus
- Zugriff auf das Firmennetzwerk von aussen nur über verschlüsselten Kanal (Virtual Private Network, VPN) und Zwei-Faktor-Authentifizierung
- Verwendung von frei zugänglichen – und teilweise auch passwortgeschützten – WLAN nur über eine VPN-Verbindung oder über das Roaming; WLAN, Bluetooth und Lokalisierungsdienste bei Nichtgebrauch deaktivieren
- Vertrauliche Dokumente weder im Hotelzimmer noch im Zimmersafe aufbewahren
- Bei Einreise das Mobiltelefon erst nach der Grenzkontrolle einschalten; bei Ausreise vor der Ausreisekontrolle ausschalten
- Vorsicht bei Kontaktversuchen, Einladungen und teuren Geschenken (Gegenleistung)

Bei Verdacht auf Spionage

- Indizien sichern
- Vorfall schnellstmöglich melden:
  - bei der Kantonspolizei
  - beim Nachrichtendienst des Bundes (*www.ndb.admin.ch*)

Der NDB wertet Hinweise aus und garantiert eine diskrete Behandlung des Spionagefalls.

Weiterführende Links

- **Dossier Wirtschaftsspionage:** *www.ndb.admin.ch/wirtschaftsspionage*
  - **Prophylax**: Präventions- und Sensibilisierungsprogramm des NDB zu den von Spionage und Proliferation ausgehenden Bedrohungen (Broschüre unter *www.ndb.admin.ch/prophylax*)
  - **Sensibilisierungsfilm** über Spionage ***„Im Visier"*** sowie **Erläuterungen** zu den gezeigten Spionagemethoden und entsprechende Schutzmassnahmen
  - verschiedene **Merk- und Faktenblätter** zu den Themen Spionage und Proliferation
- Für Fragen oder Informationen zum Programm Prophylax: *prophylax@ndb.admin.ch*
- Melde- und Analysestelle Informationssicherung: *www.melani.admin.ch*
- Meldung von Phishing-E-Mails und Phishing-Seiten: *www.antiphishing.ch*