Röhl, André; Starz, Philipp

Working Paper

Wirtschaftsschutz in der digitalen Ära – Resilienzmanagement und proaktive Open Source Intelligence als Mittel der Wahl

Working Paper des Studiengangs Sicherheitsmanagement an der NBS Northern Business School Hamburg, No. 1/2024

Provided in Cooperation with:
NBS Northern Business School – University of Applied Sciences, Hamburg

Suggested Citation: Röhl, André; Starz, Philipp (2024) : Wirtschaftsschutz in der digitalen Ära – Resilienzmanagement und proaktive Open Source Intelligence als Mittel der Wahl, Working Paper des Studiengangs Sicherheitsmanagement an der NBS Northern Business School Hamburg, No. 1/2024, NBS Northern Business School - University of Applied Sciences, Hamburg

This Version is available at:
https://hdl.handle.net/10419/294879

Working Paper des Studiengangs Sicherheitsmanagement
an der NBS Northern Business School Hamburg

Institute for Intelligence and Security Management (I2SM)

No. 1/ 2024

Wirtschaftsschutz in der digitalen Ära – Resilienzmanagement und proaktive Open Source Intelligence als Mittel der Wahl

Röhl, André & Starz, Philipp

Zusammenfassung

Die zunehmenden geopolitischen Spannungen, vor allem durch den Konflikt zwischen Russland und der Ukraine, stellen Deutschland und seine Unternehmen vor eine komplexe Bedrohungslage, die mit erhöhten Risiken aufgrund von Sabotageaktivitäten und Wirtschaftsspionage einhergeht. Vor diesem Hintergrund stehen deutsche Unternehmen vor erheblichen Herausforderungen, die eine proaktive und wachsame Herangehensweise erfordern, um die damit verbundenen Risiken zu mindern. Trotz der vielfältigen Herausforderungen bietet die heutige vernetzte digitale Landschaft Unternehmen auch technologische Möglichkeiten, ihre Abwehrmechanismen zu stärken und sich proaktiv vor potenziellen Bedrohungen zu schützen. Durch die Nutzung von Methoden und Technologien zur Datenerfassung aus mobilen Anwendungen (ADINT) können Unternehmen effektive Maßnahmen ergreifen, um ihre Sicherheit zu verbessern und sensible Daten zu schützen.[1]

Abstract

Increasing geopolitical tensions, particularly due to the conflict between Russia and Ukraine, present Germany and its companies with a complex threat situation that is accompanied by increased risks from sabotage activities and industrial espionage. Against this backdrop, German companies face significant challenges requiring a proactive and vigilant approach to minimize the associated risks. Despite the many challenges, today's interconnected digital landscape also offers companies technological opportunities to strengthen their defenses and proactively protect themselves from potential threats. By utilizing methods and technologies to collect data from mobile applications (ADINT), companies can take effective measures to improve their security and protect sensitive data.

.

[1] Prof. Dr. André Röhl ist Leiter des Studiengangs Sicherheitsmanagement an der NBS Northern Business School und stellvertretender Leiter des Instituts für Intelligence and Security Management (I2SM). Philipp Starz ist Senior Business Development Manager bei Traversals Analytics and Intelligence GmbH und Research Fellow im I2SM. Vor seiner Tätigkeit bei Traversals war er Stabsoffizier in der Bundeswehr und verfügt über langjährige Auslandserfahrung und Beratungstätigkeit in Konfliktgebieten als Interkultureller Einsatzberater. Starz hat einen Bachelor-Abschluss in Politikwissenschaft von der Universität Regensburg, einen Master-Abschluss in International Relations von der Technischen Universität Dresden und einen weiteren Master-Abschluss in Civil-Military Interaction von der Helmut-Schmidt-Universität Hamburg. Sein wissenschaftliches Interesse liegt im Bereich Open Source Intelligence, Data Sources sowie der Lagebilderstellung für eine optimierte Entscheidungsfindung.

Wirtschaftsspionage und hybride Bedrohungen für die Wirtschaft

Im Frühjahr 2024 häufen sich Medienberichte über Ermittlungen gegen Personen, die der Spionage für die Volksrepublik China oder die Russische Föderation in Deutschland verdächtigt werden.[2] Dies hat auch Implikationen für die deutsche Wirtschaft und die durch sie im Kontext des Wirtschaftsschutz zu treffenden Maßnahmen.

Dabei war die Bedrohung der Wirtschaftsspionage als von staatlichen Institutionen unterstützte Form der Informationsgewinnung auch in Zeiten des „Endes der Geschichte" nie gänzlich verschwunden. Zu fließend waren gerade in Hinblick auf die Globalisierung der Wirtschaftsbeziehungen die Übergänge zwischen Unternehmen (Konkurrenzspionage) und staatlichen Wirtschaftsinteressen. Dies führte auch zu Spionageaktivitäten zwischen Staaten, die eigentlich freundschaftlich verbunden waren. Ein weiter Treiber für Wirtschaftsspionage waren neben der Umgehung von Sanktionsregimen Versuche, technologische Vorsprünge anderer aufzuholen.[3]

Die Modi Operandi von Wirtschaftsspionage und Konkurrenzausspähung sind nahezu identisch und stützen sich auf den Menschen als Aufklärungsziel (HUMINT), technische Aufklärung (TECHINT) sowie der Sammlung und Analyse von öffentlich verfügbaren Informationen (OSINT).[4]

Tabelle 1 verdeutlicht, wie sich TECHINT, HUMINT und OSINT als Mittel der Wirtschaftsspionage voneinander abgrenzen und welche spezifischen Eigenschaften, Risiken, Einsatzarten und rechtliche Rahmenbedingungen sie jeweils mit sich bringen.

[2] Vgl. u.a. Bewarder, Manuel; Flade, Florian & Milling, Palina (2024): Wie Russland seine Spionage umstellt, https://www.tagesschau.de/investigativ/ndr-wdr/spionage-russland-deutschland-100.html; Rohde, Christian (2024): Jan Marsalek koordinierte Spionageaktionen, 10.04.2024, https://www.zdf.de/nachrichten/politik/jan-marsalek-chats-spionage-russland-wirecard-100.html; FAZ (2024): Krahs Büro soll geheime Dokumente abgerufen haben, 27.04.2024, https://www.faz.net/aktuell/politik/ausland/krahs-buero-rief-geheime-dokumente-im-handelsausschuss-ab-19683026.html.; Bartlett-Imadegawa, Rhyannon & Kastner, Jens (2024): China spy suspects in U.K. and Germany seen as ‚tip of iceberg', https://asia.nikkei.com/cms/Politics/Defense/China-spy-suspects-in-U.K.-and-Germany-seen-as-tip-of-iceberg.

[3] Vgl. BfV (Hg.) (2014): Wirtschaftsspionage – Risiko für Unternehmen, Wissenschaft und Forschung, https://www.wirtschaftsschutz.info/SharedDocs/Publikationen/DE/Spionage/Wirtschaftsspionage_Risiken.html, S.5ff.

[4] Vgl. Wallwaey, Elisa; Esther Bollhofer & Susanne Knickmeier (2020) (Hg.): Wirtschaftsspionage und Konkurrenzausspähung: Phänomenologie, Strafverfolgung und Prävention in ausgewählten Europäischen Ländern. Berlin: Duncker & Humblot, S.28f.

Tabelle 1: Unterschiede zwischen TECHINT, HUMINT und OSINT als Mittel der Wirtschaftsspionage.[5] Eigene Darstellung.

Aspekt	TECHINT	HUMINT	OSINT
Definition	Nutzung technischer Mittel wie Überwachung, Hacking, Abhören von Kommunikation, um Informationen zu erhalten.	Gewinnung von Informationen durch direkten Kontakt mit Personen, z.B. Informanten, Mitarbeiter oder Geschäftspartner.	Sammlung von Informationen aus öffentlich zugänglichen Quellen wie Internet, Medienberichten, sozialen Medien usw.
Beispiele	Hacking von Unternehmensnetz-werken, Überwachung von Kommunikations-systemen, Diebstahl von geistigem Eigentum über digitale Kanäle.	Rekrutierung von Mitarbeitern oder Informanten in Unternehmen, Informationsaustausch auf Konferenzen oder in informellen Treffen.	Analyse von Unternehmenswebsites, Social-Media-Posts von Mitarbeitern, öffentliche Aussagen von Führungskräften.
Risiken	Gesetzwidrigkeit, hohe technische Fähigkeiten erforderlich, Entdeckungsgefahr durch Sicherheitsmaßnahmen	Abhängigkeit von der Zuverlässigkeit von Informanten, ethische Bedenken bei der Informationsbeschaffung, Risiko der Enttarnung der Quelle.	Abhängigkeit von der Verfügbarkeit und Genauigkeit öffentlicher Informationen, Schwierigkeiten bei der Interpretation und Analyse großer Datenmengen.
Einsatzgebiet	Technologieunternehmen, Forschungseinrichtungen mit hochtechnologischen Entwicklungen.	Alle Unternehmen, insbesondere solche mit sensiblen Geschäftsgeheimnissen oder strategischen Informationen.	Unternehmen jeglicher Art, da Informationen aus öffentlichen Quellen leicht zugänglich sind.
Legalität	Oft illegal und als Verstoß gegen Datenschutzgesetze betrachtet.	Legale Methoden, solange sie ethisch und unter Einhaltung von Datenschutzrichtlinien durchgeführt werden.	Legal, da Informationen aus öffentlichen Quellen stammen und frei verfügbar sind.
Zugang	Compelled Acces	Direct Access	Non-Compelled Access

Ab den 2000er Jahren stellte Technologie schließlich nicht nur ein Ziel von Spionageaktivitäten dar, sondern erweiterte durch die voranschreitende Digitalisierung auch exponentiell die Möglichkeiten, Informationen zu gewinnen. Nicht außer Acht gelassen werden sollte jedoch, dass Wirtschaftsspionage nicht allein aus konspirativen Aktivitäten bestehen muss. Die sogenannte offene Beschaffung (Open Source Intelligence) bietet durch Auswertung öffentlich verfügbarer Daten, häufig aus der Eigendarstellung von Unternehmen und Mitarbeiter in unterschiedlichen sozialen Medien, viele legale Anknüpfungspunkte für weitere gezielte Maßnahmen. Auch hier bietet die Digitalisierung, insbesondere über Big Data-Analysen, Angreifern neue Möglichkeiten.[6]

[5] Vgl. Ebenda, S.28f.

[6] Die qualitative Veränderung der Risikolandschaft durch die Digitalisierung stellt aus Sicht des Sicherheitsmanagements anschaulich das „Sicherheitsvisier“ dar, in dem die Veränderungen durch

Betroffenen Unternehmen ist dabei zunächst häufig der Wert, der über die offene Beschaffung erlangten Informationen, nicht bewusst. Ihre Bedeutung ergibt sich unter Umständen erst durch Verknüpfung mit der weiterführenden Manipulation von Mitarbeitern (Social Engineering) oder dem Einsatz weiterer konspirativer Maßnahmen wie Abhörmaßnahmen, Diebstahl oder Cyberangriffen.

Es kann davon ausgegangen werden, dass es im Hinblick auf die in den letzten Jahren zunehmende Cyberkriminalität Überschneidungen mit der Wirtschaftsspionage gibt. Kriminelle Organisationen mit einem hohen Professionalisierungsgrad wurden möglicherweise von interessierten Staaten geduldet oder aktiv in die eigenen Spionageaktivitäten eingebunden, um eine eigene Beteiligung zu verschleiern.[7]

Auch aufgrund dieser Überschneidungen ist es schwierig, den tatsächlichen Umfang der Wirtschaftsspionage gegen die deutsche Wirtschaft und den daraus explizit für die Unternehmen und die Volkswirtschaft entstehenden Schaden zu beziffern. Hinzu kommen die allgemeinen Herausforderungen bei der statistischen Erfassung von Kriminalität gegen Unternehmen.[8]

Im Rahmen des Forschungsprojekts WISKOS (2015-2017) gaben von den befragten deutschen KMU 45% an, in den letzten 5 Jahren mindestens einen Verdachtsfall auf Konkurrenzspionage oder Wirtschaftsspionage gehabt zu haben. Rund ein Viertel der befragten KMU gab an, dass diese Vorfälle eine Betriebsunterbrechung von mindestens 48 Stunden zur Folge gehabt hätten. Konkrete Schadenssummen konnten nicht abgeleitet werden.[9] Im Rahmen der Bitkom-Studie Wirtschaftsschutz 2023 gaben 72% der befragten Unternehmen an, nach eigener Wahrnehmung in den letzten 12 Monaten von Diebstahl, Industriespionage oder Sabotage betroffen gewesen zu sein. Dies sei mit einem Schaden von rund 205,9 Mrd. EUR verbunden gewesen. Beide Werte waren in den Vorjahren sogar noch höher (2021: 88% / 223,5 Mrd. EUR).[10]

Als vermutliche Ursprungsländer wurden in der Bitkom-Studie durch die Befragten vorrangig die Volksrepublik China (42%) und die Russische Föderation (46%) benannt.[11] Beide Länder

---

Unterscheidung digitaler und analoger, globaler und lokaler Angriffsvektoren deutlich werden. Vgl. ASW-Bundesverband (Hg.) (2019): #DESINFORMATION, Studie, https://asw-bundesverband.de/wp-content/uploads/studie_desinformation_web_v3.pdf, S.18f.

[7] Vgl. BfV (2018): Nachrichtendienstlich gesteuerte Cyberangriffe, https://www.wirtschaftsschutz.info/SharedDocs/Publikationen/DE/IT_EA/Nachrichtendienstlich_gesteuerte_Cyberangriffe.pdf?__blob=publicationFile&v=4, S.20.

[8] Vgl. Schulz, André (2023): Wirtschaftskriminalität im Schatten der Pandemie - Unternehmen und die Gefahr einer dritten Krise (Fortschreibung), Working Paper des Studiengangs Sicherheitsmanagement an der NBS Northern Business School Hamburg, No. 1/2023, https://hdl.handle.net/10419/273461, S.4f.

[9] Vgl. Wallwaey, Elisa (o.J.): Wirtschaftsspionage, Konkurrenzausspähung – Das Forschungsprojekt WISKOS / Die Ergebnisse im Überblick, o.O., S.1ff.

[10] Vgl. Wintergerst, Ralf (2023): Wirtschaftsschutz 2023, Studie, https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf, S.3f.

[11] Vgl. ebenda, S.5.

werden regelmäßig auch durch den Bundesverfassungsschutz als maßgebliche Bedrohungen im Zusammenhang mit Wirtschaftsspionage benannt.[12]

Die Volksrepublik China verfügt heute mutmaßlich über die umfangreichsten nachrichtendienstlichen Strukturen der Welt und strebt eine globale Rolle als ökonomische und technologische Führungsmacht an.[13] Hinzu kommt ein „Whole-of-state"[14]-Ansatz, dem zufolge alle Behörden, Unternehmen und Staatsbürger in die Aktivitäten der Wirtschaftsspionage eingebunden werden können. Verbindendes Element ist hierbei die Rolle der Kommunistischen Partei in Staat, Wirtschaft und Gesellschaft, vergleichbar in Teilen mit den betrieblichen Parteistrukturen der Sozialistischen Einheitspartei Deutschlands (SED) in der DDR.[15] In der Folge können auch unscheinbare Informationen durch Kombination mit einer Vielzahl von anderen Daten und technischen Auswertungen zu aussagekräftigen Lagebildern führen.[16]

Die Russische Föderation verfolgt seit Jahren eine aggressivere Außenpolitik, was durch eine Verstärkung nachrichtendienstlicher Aktivitäten begleitet wird. Letztere befänden sich heute in Deutschland wieder auf dem Niveau des Kalten Krieges.[17] Der andauernde Krieg gegen die Ukraine führt zu einer Konfrontation mit den Staaten der Europäischen Union und der NATO. Jenseits eines erweiterten Interesses der Russischen Föderation an Wirtschaftsspionage zur Umgehung der Sanktionen, sehen sich Unternehmen in Deutschland daher auch den Auswirkungen hybrider Bedrohungen gegenüber und insbesondere Organisationen, die im weiteren Sinne als Kritische Infrastrukturen betrachtet werden können, sind der Gefahr der Manipulation bis hin zur Sabotage ausgesetzt.[18]

Dieser Trend zur Gefährdung von Unternehmen infolge hybrider Bedrohungen stellt nach der vielschichtigen Veränderung durch die Digitalisierung die zweite maßgebliche qualitative Veränderung im Bedrohungskontext des Wirtschaftsschutzes dar. Unternehmen müssen Maßnahmen ergreifen, um die daraus entstehenden Risiken ganzheitlich zu adressieren.

---

[12] Vgl. BfV (Hg.) (2014): Wirtschaftsspionage – Risiko für Unternehmen, Wissenschaft und Forschung, https://www.wirtschaftsschutz.info/SharedDocs/Publikationen/DE/Spionage/Wirtschaftsspionage_Risiken.html, S.8ff.; Wirtschaftsschutz BfV (2023): Sicherheit versus Freiheit, in: Single Point of Contact, No. 2/2023, S.8ff.

[13] Vgl. Intelligence and Security Commiittee of Parliament (2023): China, https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf, S.11f.

[14] Ebenda, S.30.

[15] Vgl. Ebenda, S.30.

[16] Siehe auch die Empfehlungen an deutsche Hochschulen zur Forschungszusammenarbeit mit der Volksrepublik China, z.B. Gillmann, Barbara (2022): ‚Man darf nicht naiv sein' – Forschungsministerin rät Hochschulen zu radikalem Schritt gegen China, https://www.handelsblatt.com/politik/deutschland/bettina-stark-watzinger-im-interview-man-darf-nicht-naiv-sein-forschungsministerin-raet-hochschulen-zu-radikalem-schritt-gegen-china/28430930.html.

[17] Vgl. Wirtschaftsschutz BfV (2023): Sicherheit versus Freiheit, in: Single Point of Contact, No. 2/2023, S.11.

[18] Vgl. Carstens, Peter (2024): ‚Im Frieden befinden wir uns schon lange nicht mehr', Interview mit GL André Bodemann, https://www.faz.net/aktuell/politik/inland/operationsplan-deutschland-warum-es-im-ernstfall-auf-jeden-buerger-ankommt-19669372.html.; siehe auch: Barkóciová, Miroslava; Mihalčová, Bohuslava; Černák, Filip & Šišulák, Stanislav (2023): Hybrid threats and their impact on the performance of the business environment, in: Entrepreneurship and Sustainability Issues, 11(2), http://doi.org/10.9770/jesi.2023.11.2(31), S.466-479.

Maßnahmen des Wirtschaftsschutzes aus Unternehmensperspektive – das Resilienzmodell

Der in den letzten Jahren in vielen Fachdisziplinen diskutierte Ansatz der Resilienzförderung bietet im Sinne einer organisationellen Krisenresilienz für den Wirtschaftsschutz die Möglichkeit einer Systematisierung erforderlicher Maßnahmen. Die organisationelle Krisenresilienz kann dabei unterteilt werden in Fähigkeiten zur Verhinderung von Schadensereignissen (Widerstandsfähigkeit) und Fähigkeiten zum Umgang mit Schadensereignissen (Bewältigungsfähigkeit). Zusätzlich können die Maßnahmen danach unterschieden werden, ob sie innerhalb und explizit für die eigene Organisation erfolgen (inneres Ökosystem) oder ob sie auf Vernetzungen und gemeinschaftliche Handlungen abzielen (äußeres Ökosystem).[19]

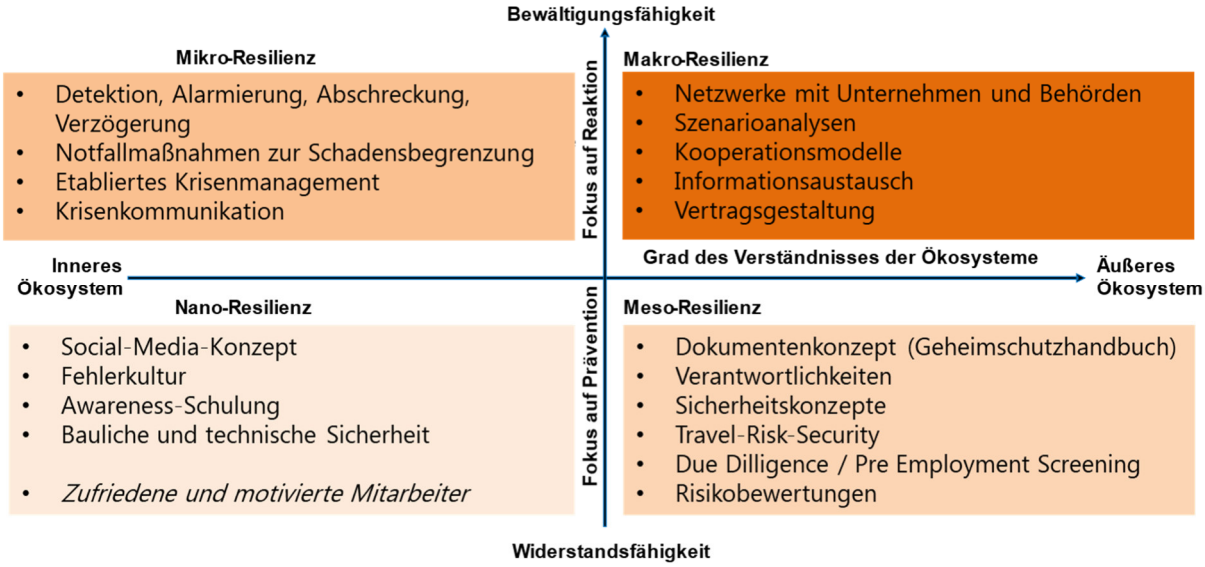


Abbildung 1: Resilienzmodell (Kerstan & Röhl 2022) mit Wirtschaftsschutzmaßnahmen.

Wird dieses Resilienzmodell zugrunde gelegt, lassen sich unterschiedliche Anforderungen an den Wirtschaftsschutz eines Unternehmens ableiten. Im Mittelpunkt steht dabei immer, dass es ein Verständnis dafür gibt, welche Informationen und welche Prozesse im Unternehmen besonders schützenwert sind.

Im Zusammenhang mit der Nano-Resilienz (Widerstandsfähigkeit / Inneres Ökosystem, Fokus auf Prävention) können insbesondere Maßnahmen zur bewussten oder unbewussten Täterschaft der Mitarbeiter formuliert werden. Dies umfasst sowohl Awareness Schulungen, eine offene Fehlerkultur zum rechtzeitigen Entdecken von Abweichungen sowie die Förderung von Motivation und Zufriedenheit bei den Mitarbeitern, um Komplizenschaft aus Frustration

[19] Vgl. Kerstan, R. & Röhl, A. (2022): Die Bedeutung organisationaler Ökosysteme für den Erfolg der Unternehmenssicherheit, in: Endreß, Hennies, Peters & Vogt (Hg.): Wirtschaftsschutz in der Praxis – Herausforderungen an die Sicherheit im Zeitalter von Digitalisierung und Krise, Springer, S.200ff.

o.ä. zu vermeiden. Zugleich können durch ein angepasstes Social-Media-Konzept und Maßnahmen der baulichen und technischen Sicherheit die Risiken für einen Informationsabfluss verringert werden.[20]

Die Mikro-Resilienz (Bewältigungsfähigkeit / Inneres Ökosystem, Fokus auf Reaktion) basiert auf einer zeitnahen Feststellung, dass es den Versuch von Spionage oder Sabotage gibt. Hierzu müssen Prozesse der Detektion und Alarmierung im weiteren Sinne ebenso etabliert werden wie ein wirksames Krisenmanagement.

Bei der Meso-Resilienz (Widerstandsfähigkeit / Äußeres Ökosystem, Fokus auf Prävention) geht es um die eindeutige Festlegung von Schutzzielen, Verantwortlichkeiten und den dazugehörigen Konzepten. Dazu zählen Maßnahmen der Due Dilligence gegenüber anderen Organisationen ebenso wie ein Pre-Employment Screening bei Stellen mit einer besonderen Verantwortung. Ebenso sind geeignete Maßnahmen für Geschäftsreisen zu identifizieren.

Die Makro-Resilienz (Bewältigungsfähigkeit / Äußeres Ökosystem, Fokus auf Reaktion) basiert auf der Zusammenarbeit mit den zuständigen Behörden wie Bundesverfassungsschutz und Landesverfassungsschutz sowie der Teilnahme an den Initiativen des Wirtschaftsschutzes[21] und ermöglicht ein aktuelles Bedrohungslagebild, Beratung im Bedarfsfall sowie ggf. auch Kooperationen zwischen Unternehmen.

Maßnahmen des Wirtschaftsschutzes aus Unternehmensperspektive – Advertising-based Intelligence und Open Source Intelligence

Technologische Veränderungen führen nicht nur zu einer erhöhten Vulnerabilität von Unternehmen gegenüber Wirtschaftskriminalität, sie bieten den Unternehmen auch die Möglichkeit proaktiv Maßnahmen zum Schutz ihrer Daten und ihres geistigen Eigentums zu ergreifen. Eine Möglichkeit besteht in der Nutzung von Advertising-based Intelligence (ADINT) in Kombination mit OSINT.

ADINT ist das Sammeln von Informationen durch den Kauf von Werbedaten. ADINT nutzt dabei die umfangreichen Datenströme, die durch werbefinanzierte mobile Anwendungen generiert werden, um Einblicke in das Nutzerverhalten zu gewinnen. Diese Anwendungen sammeln Standortdaten und andere Informationen der Nutzer, um sie an Datenbroker und Werbepartner weiterzugeben. ADINT ermöglicht es, diese Daten zu analysieren und Muster zu erkennen, die auf potenzielle Bedrohungen oder Risiken hinweisen könnten.

Zum Beispiel könnten ungewöhnliche Aktivitäten oder verdächtige Verbindungen zwischen verschiedenen Nutzern oder Geräten auf eine mögliche Wirtschaftsspionage hinweisen. Das Herzstück vieler mobiler Anwendungen ist die Datenerfassung, insbesondere in Bezug auf die Standortdaten der Nutzer. Mobile Apps enthalten oft Software Developer Kits (SDKs), um

[20] Siehe auch: Mészáros, Alexandra Agnes & Kelemen-Erdős, Aniko (2023): Industrial espionage from a human factor perspective, in: Journal of International Studies, 16(3), doi:10.14254/2071-8330.2023/16-3/5, S.97-116.
[21] Z.B. www.wirtschaftsschutz.info

Standortdaten zu sammeln und an Datenbroker und Werbepartner zu übermitteln. Werbetreibende sammeln Daten über Nutzer und ihre Mobilgeräte durch Anzeigen, die in Android- und iOS-Apps geschaltet werden. In den meisten Fällen werden dabei Standort-, Geräte- und App-Informationen über eine eindeutige Mobile Advertising-ID (MA-ID) mit demselben Gerät verknüpft. Die MA-ID ist eine Folge von Symbolen, die vom Betriebssystem des Mobilgeräts vergeben wird. Sie wird mit den Servern der Apps geteilt, die der Nutzer verwendet, um seine Reise zu verfolgen und seine Entscheidungen zu treffen. Die MA-ID auf Android Google Ad ID (GAID) und iOS (IDFA) sind Teil der Betriebssysteme und wurden in den letzten Jahren entsprechend den aktualisierten Datenschutzrichtlinien geändert. Wenn die MA-ID nicht verfügbar ist, können Werbetreibende dennoch Geokoordinaten oder IP-Adressen verwenden, um aus Daten, die von verschiedenen Anzeigenplatzierungen gesammelt wurden, Verbindungen abzuleiten.

Durch die Nutzung werbefinanzierter mobiler Anwendungen erlauben die Nutzer die Datenschutz-Grundverordnung (DSGVO)-konforme Weitergabe feinkörniger Informationen an Hunderte von Unternehmen im Werbe-Ökosystem. Dieser "Bidstream" von Informationen kann von verschiedenen Stellen, einschließlich Regierungsbehörden, böswilligen Akteuren aber auch zur Gegenaufklärung für eigene Absichten weiterverwendet werden.

Solche Analysewerkzeuge helfen bei der Gewinnung neuer Informationen durch Kombination und Kreuzanalyse mehrerer Datensätze. Sie können besonders wichtig sein, wenn interne Daten mit kommerziell erworbenen Daten und OSINT kombiniert werden. Es ist sehr wahrscheinlich, dass andere Sicherheits- und Nachrichtendienste in ganz Europa in erheblichem Maße auf gekaufte Daten sowie auf sehr weit gefasste Open-Source-Informationen zurückgreifen.[22]

Unternehmen können ADINT und OSINT nutzen, um Informationen über potenzielle Bedrohungen oder Risiken aus öffentlichen Quellen zu sammeln und zu analysieren. Dies kann helfen, Muster zu identifizieren und Frühwarnungen für mögliche Angriffe zu geben.

Anwendungsbeispiel Geofencing der Traversals Analytics and Intelligence GmbH[23]

Geofencing ist eine Technologie, die es Unternehmen ermöglicht, virtuelle Grenzen um bestimmte geografische Gebiete zu ziehen und automatisch Aktionen auszulösen, wenn ein Gerät, das in Verbindung mit Spionageaktivitäten gebracht worden ist, in diesen Bereich eintritt oder ihn verlässt. Im Kontext des Wirtschaftsschutzes gewinnt diese Technologie an

[22] Vgl. Wetzling, Thorsten & Dietrich, Charlotte (2022): Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform?, Stiftung Neue Verantwortung, doi: 10.13140/RG.2.2.15489.74080, S. 10.

[23] Traversals Analytics and Intelligence GmbH ist ein deutsches Technologie-Unternehmen, dass sich auf die Lagebilderstellung und die Unterstützung des Krisenmanagements in Unternehmen, staatlichen Institutionen und Hilfsorganisationen durch innovative Ansätze in der Anwendung Künstlichen Intelligenz konzentriert. traversals.com.

Bedeutung, insbesondere wenn es darum geht, potenzielle Spionageaktivitäten zu erkennen und zu verhindern.

Es kann davon ausgegangen werden, dass Spionageaktivitäten ungeachtet der Vielschichtigkeit der verwendeten Methoden zu einem großen Teil an die Verknüpfung mit als Geoentitäten beschreibbaren Orten in einem Zielland gebunden sind. Bei diesen Geoentitäten handelt es sich um Örtlichkeiten, in denen sich nachrichtendienstlich aktive Personen aufhalten können, z.B. Botschaften, Konsulate, geschäftliche Niederlassungen.[24]

Durch Verknüpfung von ADINT-Daten mit relevanten Geoentitäten sowie Monitoring und Analyse von Standortdaten können Unternehmen verdächtige Aktivitäten oder Muster identifizieren, die auf Spionageaktivitäten hinweisen könnten. Wenn beispielsweise ein Gerät wiederholt in der Nähe von Unternehmensstandorten, Produktionsstätten oder Forschungseinrichtungen lokalisiert wird, könnte dies ein Anzeichen für Spionageaktivitäten sein. Bei Erkennung von verdächtigen Standortdaten können automatische Warnmeldungen an Sicherheitspersonal oder Entscheidungsträger gesendet werden.

Geofencing in Verbindung mit dem Monitoring von Standortdaten ermöglicht damit eine schnelle Reaktion und kann dabei helfen, potenzielle Bedrohungen durch Spionage oder gar Sabotage frühzeitig zu erkennen und entsprechende Sicherheitsmaßnahmen einzuleiten. Geofencing kann auch genutzt werden, um den Zugang zu sensiblen Unternehmensbereichen oder -gebäuden zu beschränken. Sobald verdächtige Aktivitäten erkannt werden, können automatische Maßnahmen ausgelöst werden, wie zum Beispiel die Aktivierung zusätzlicher Sicherheitsprotokolle oder die Benachrichtigung des Sicherheitspersonals.

Durch Einbindung spezialisierter Dienstleister können folgende Maßnahmen kombiniert werden:

1. Erkennung ungewöhnlicher Aktivitäten:

   Durch die Analyse von Standortdaten können Unternehmen ungewöhnliche Bewegungsmuster oder wiederkehrende Besuche in der Nähe von Unternehmensstandorten oder sensiblen Einrichtungen identifizieren. Zum Beispiel könnten wiederholte oder unerwartete Besuche in der Nähe von Forschungseinrichtungen oder Produktionsstätten auf verdächtige Aktivitäten hinweisen. Unternehmen können diese Informationen nutzen, um potenzielle Spionageaktivitäten frühzeitig zu erkennen und angemessen zu reagieren, indem sie zusätzliche Sicherheitsmaßnahmen implementieren oder entsprechende Behörden informieren.

2. Überprüfung der Authentizität von angeblichen Diplomaten oder Journalisten:

   Unternehmen können die Aktivitäten von Personen, die angeblich als Diplomaten oder Journalisten tätig sind, überprüfen, indem sie ihre Standortdaten analysieren

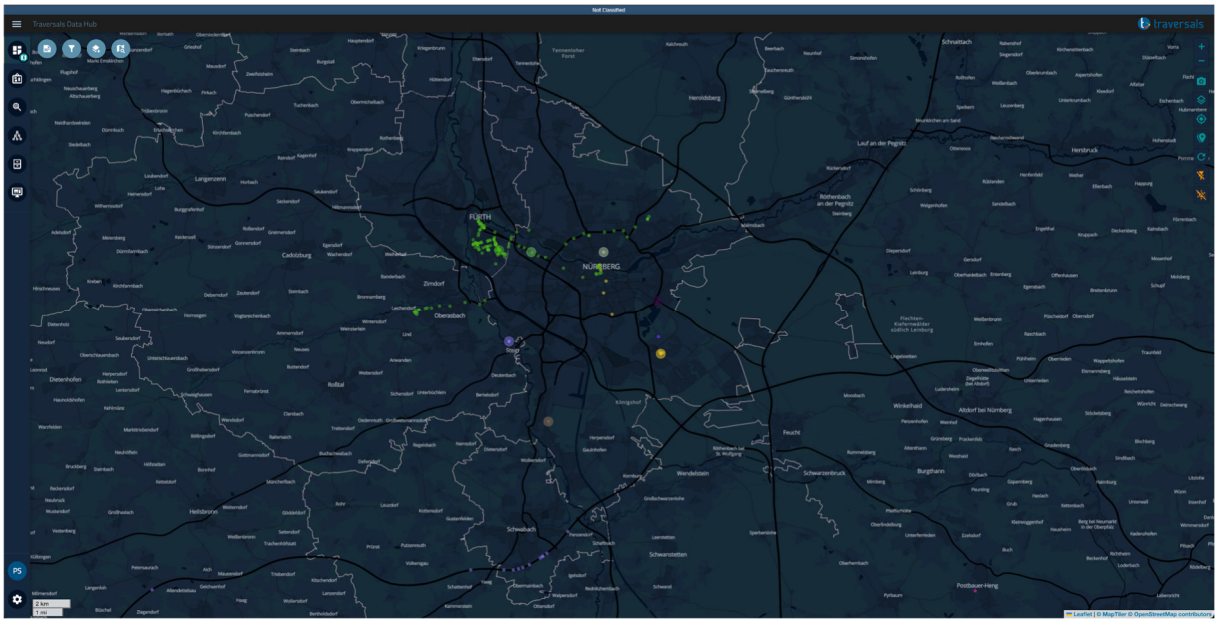
[24] Vgl. BMI (o.J.): Abwehr von Spionageaktivitäten in Deutschland, https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/spionage/spionage-artikel.html#Arbeits-%20und%20Vorgehensweise%20Fremder%20Dienste.

und mit offiziellen Datenbanken oder öffentlich verfügbaren Informationen abgleichen (OSINT). Wenn die Standortdaten einer Person nicht mit ihren offiziellen Aufgaben oder Aktivitäten übereinstimmen, könnte dies auf eine mögliche Tarnung oder unangemessene Aktivitäten hinweisen. In solchen Fällen können Unternehmen geeignete Maßnahmen ergreifen, um die Authentizität der betreffenden Personen zu überprüfen oder verdächtige Aktivitäten zu melden.

3. Früherkennung von potenziellen Bedrohungen:

   Durch die kontinuierliche Überwachung und Analyse von Unternehmensstandortdaten können Unternehmen potenzielle Spionageaktivitäten frühzeitig erkennen und entsprechende interne Sicherheitsmaßnahmen ergreifen oder dies an die verantwortlichen Behörden melden. Die Analyse von Standortdaten in Echtzeit ermöglicht es Unternehmen, verdächtige Aktivitäten oder Muster zu identifizieren, die auf Spionageaktivitäten hinweisen könnten, und sofortige Maßnahmen zu ergreifen, um potenzielle Risiken zu minimieren oder zu beseitigen.

Abbildung 2: Sanitarisierte Darstellung von Bewegungsmustern in der Metropolregion Nürnberg Traversals Analytics and Intelligence GmbH.



Fazit

Unternehmen sehen sich im Zusammengang mit Wirtschaftsspionage und Sabotage einem zweifach qualitativ verstärkten Bedrohungskontext gegenüber. Sowohl technologische Entwicklungen der Digitalisierung als auch die Verstärkung hybrider Bedrohungen erhöhen das Risikopotential.

Die Unternehmen sind dieser Bedrohung durch staatliche Akteure jedoch nicht hilflos ausgeliefert. Durch systematische Umsetzung einschlägiger resilienzfördernder Maßnahmen kann die Widerstandsfähigkeit gestärkt und die Bewältigungsfähigkeit gefördert werden. Durch Kooperationen, den Einsatz von spezialisierten Dienstleistern und Nutzung technologischer Möglichkeiten können insbesondere die Detektion von Spionage- und Sabotageversuchen deutlich verbessert werden.

Quellen- und Literaturverzeichnis[25]

ASW-Bundesverband (Hg.) (2019): #DESINFORMATION, Studie, https://asw-bundesverband.de/wp-content/uploads/studie_desinformation_web_v3.pdf.

Barkóciová, Miroslava; Mihalčová, Bohuslava; Černák, Filip & Šišulák, Stanislav (2023): Hybrid threats and their impact on the performance of the business environment, in: Entrepreneurship and Sustainability Issues, 11(2), http://doi.org/10.9770/jesi.2023.11.2(31), S.466-479.

Bartlett-Imadegawa, Rhyannon & Kastner, Jens (2024): China spy suspects in U.K. and Germany seen as ‚tip of iceberg', https://asia.nikkei.com/cms/Politics/Defense/China-spy-suspects-in-U.K.-and-Germany-seen-as-tip-of-iceberg.

Bewarder, Manuel; Flade, Florian & Milling, Palina (2024): Wie Russland seine Spionage umstellt, https://www.tagesschau.de/investigativ/ndr-wdr/spionage-russland-deutschland-100.html.

BMI (o.J.): Abwehr von Spionageaktivitäten in Deutschland, https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/spionage/spionage-artikel.html#Arbeits-%20und%20Vorgehensweise%20Fremder%20Dienste.

BfV (Hg.) (2014): Wirtschaftsspionage – Risiko für Unternehmen, Wissenschaft und Forschung, https://www.wirtschaftsschutz.info/SharedDocs/Publikationen/DE/Spionage/Wirtschaftsspionage_Risiken.html

BfV (2018): Nachrichtendienstlich gesteuerte Cyberangriffe, https://www.wirtschaftsschutz.info/SharedDocs/Publikationen/DE/IT_EA/Nachrichtendienstlich_gesteuerte_Cyberangriffe.pdf?__blob=publicationFile&v=4.

Carstens, Peter (2024): ‚Im Frieden befinden wir uns schon lange nicht mehr', Interview mit GL André Bodemann, https://www.faz.net/aktuell/politik/inland/operationsplan-deutschland-warum-es-im-ernstfall-auf-jeden-buerger-ankommt-19669372.html.

Intelligence and Security Commiittee of Parliament (2023): China, https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf.

FAZ (2024): Krahs Büro soll geheime Dokumente abgerufen haben, 27.04.2024, https://www.faz.net/aktuell/politik/ausland/krahs-buero-rief-geheime-dokumente-im-handelsausschuss-ab-19683026.html.

Gillmann, Barbara (2022): ‚Man darf nicht naiv sein' – Forschungsministerin rät Hochschulen zu radikalem Schritt gegen China, https://www.handelsblatt.com/politik/deutschland/bettina-stark-watzinger-im-interview-

[25] Onlinequellen Stand 02.05.2024.

man-darf-nicht-naiv-sein-forschungsministerin-raet-hochschulen-zu-radikalem-schritt-gegen-china/28430930.html.

Kerstan, R. & Röhl, A. (2022): Die Bedeutung organisationaler Ökosysteme für den Erfolg der Unternehmenssicherheit, in: Endreß, Hennies, Peters & Vogt (Hg.): Wirtschaftsschutz in der Praxis – Herausforderungen an die Sicherheit im Zeitalter von Digitalisierung und Krise, Springer, S.189-206.

Mészáros, Alexandra Agnes & Kelemen-Erdős, Aniko (2023): Industrial espionage from a human factor perspective, in: Journal of International Studies, 16(3), doi:10.14254/2071-8330.2023/16-3/5, S.97-116.

Rohde, Christian (2024): Jan Marsalek koordinierte Spionageaktionen, 10.04.2024, https://www.zdf.de/nachrichten/politik/jan-marsalek-chats-spionage-russland-wirecard-100.html.

Schulz, André (2023): Wirtschaftskriminalität im Schatten der Pandemie - Unternehmen und die Gefahr einer dritten Krise (Fortschreibung), Working Paper des Studiengangs Sicherheitsmanagement an der NBS Northern Business School Hamburg, No. 1/2023, https://hdl.handle.net/10419/273461.

Wallwaey, Elisa (o.J.): Wirtschaftsspionage, Konkurrenzausspähung – Das Forschungsprojekt WISKOS / Die Ergebnisse im Überblick, o.O.

Wallwaey, Elisa; Esther Bollhofer & Susanne Knickmeier (2020) (Hg.): Wirtschaftsspionage und Konkurrenzausspähung: Phänomenologie, Strafverfolgung und Prävention in ausgewählten Europäischen Ländern. Berlin: Duncker & Humblot.

Wetzling, Thorsten & Dietrich, Charlotte (2022): Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform?, Stiftung Neue Verantwortung, doi: 10.13140/RG.2.2.15489.74080

Wintergerst, Ralf (2023): Wirtschaftsschutz 2023, Studie, https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf.

Wirtschaftsschutz BfV (2023): Sicherheit versus Freiheit, in: Single Point of Contact, No. 2/2023.