PROTECTIVE INTELLIGENCE

Mit innovativen Sicherheitsmaßnahmen Risiken minimieren

Lesedauer: 7 Minuten

Achtung Cyberkriminalität! Neben Politikern und Prominenten geraten vor allem Unternehmer und vermögende Familien in das Fadenkreuz. „Protective Intelligence" ist das passende Zaubermittel für den Personenschutz des 21. Jahrhunderts. Was verbirgt sich dahinter und wie kann für die analoge und digitale Sicherheit gesorgt werden?

„FBI und BKA heben Marktplatz im Darknet aus", so die Headline in den Medien Anfang Mai 2019. Neben Drogen und Waffen wurden vor allem falsche Identitäten inklusive Kontoinformationen, Email-Adressen, Passwörter und Kreditkartendetails gehandelt. Ein Risiko, das für viele nicht sichtbar und somit nicht vorhanden scheint. Das Gegenteil ist der Fall. Denn das Ausspähen kann vom heimischen Computer aus geschehen. Der moderne Ansatz zum ganzheitlichen Schutz der Privatsphäre, das Prinzip der „Protective Intelligence", kann hier ein wirksames Gegenmittel darstellen.

»Protective Intelligence geht weiter und nutzt unter anderem den Cyberraum, um Gefahren und Risiken zu erkennen.«

Protective Intelligence als ganzheitliches Schutzkonzept

Für den Begriff des „Protective Intelligence" gibt es im Deutschen keine griffige und passende Übersetzung. Der Secret Service war es, der den Ansatz in den späten 70er Jahren entwickelte. Einer Weiterentwicklung des im deutschen Sprachraum geläufigen Wortes der „Vorfeldaufklärung", bei der das Umfeld der Schutzperson (Wohnung, Feriendomizil, Schulen der Kinder, Veranstaltungen etc.) durch eigenes Personal beobachtet wird, um so zu erkennen, ob diese Objekte nicht von möglichen Gefährdern ausgespäht werden. Ein Ansatz, der im Zuge der RAF- Anschläge konzipiert wurde und mittlerweile in die Jahre gekommen ist, sofern dies die alleinige Präventionsmaßnahme darstellt. „Protective Intelligence" geht weiter und nutzt unter anderem den Cyberraum, um Gefahren mit Hilfe von Risiko Monitoring früh zu erkennen. Die Vorteile für den Täter einer digitalen Ausspähung liegen auf der Hand: Anonymität, Schwachstellenidentifikation, Bedrohung und Erpressung, ohne das geschützte Umfeld zu verlassen und analog sichtbar zu werden. Wir befinden uns also an einer Schnittstelle zwischen digitaler und analoger Welt – und gleichzeitig in einem Informationskreislauf. „Protective Intelligence" ist somit das Identifizieren, Aufbereiten, Bereitstellen und Bewerten von Informationen aus Tätersicht unter Nutzung aller rechtlich zulässigen Verfahren und Quellen, um so die Grundlage für ein ganzheitliches Schutzkonzept erarbeiten zu können. Die Bewertung der gesammelten Informationen müssen dabei geschulte Analysten vornehmen, um eine Risikobeurteilung erstellen zu können. Auf dieser ruht wiederum der Maßnahmenplan. Dabei ist „Protective Intelligence"

In *aspekte* bereiten die Wealth-Management-Kompetenzzentren gemeinsam mit Netzwerkpartnern Themen auf, die für Sie relevant sind.
www.berenberg.de/unternehmer

Von Oliver Schneider, Geschäftsführender Gesellschafter der RiskWorkers GmbH und Dennis Hummelmeier, Leiter des Kompetenzzentrums Unternehmer, Berenberg

Sie haben Fragen?
Kontaktieren Sie uns gern:
Kompetenz_Unternehmer@berenberg.de

► Unternehmer
Stiftungen
Family Offices

nicht auf Personen begrenzt. Man kann es auch zum Schutz von Veranstaltungen, Gebäuden, kritischer Infrastruktur, Daten und Produkten einsetzen.

Digitales Risikomanagement

Mittlerweile versuchen immer mehr Dienstleister, die sich auf das Sammeln von Informationen spezialisiert haben und oft aus dem Bereich der Markenbeobachtung oder dem Online-Reputationsmanagement kommen, das Thema aufzugreifen. Ihre Programme können nach Schlagwörtern suchen. Doch sind sie auch in der Lage, aus Tätersicht zu denken und die Quellen zu nutzen, die Täter mittlerweile nutzen können? Die maschinelle Suche kommt ganz schnell an ihre Grenzen, wenn man Verknüpfungen und Hinweise suchen muss, die eben nur der Mensch erkennen kann. Ein praktisches Beispiel: Die Kinder eines Vorstandsvorsitzenden sind im Umgang mit Social Media geschult. Es existieren keine Social-Media-Profile und der 14-Jährige Sohn ist sonst auch nicht „auffällig". Tatsächlich lässt sich kein User auf den gängigen Plattformen finden. Allerdings gibt es einen „versteckten Account", da der Teenager einfach seinen Vornamen und Nachnamen rückwärts buchstabiert hat und so einen etwas ungewöhnlichen Namen hatte, der aber im Freundeskreis bekannt war. Das findet zunächst keine Suchmaschine. Es wäre auch nicht weiter bedenklich gewesen, wenn nicht Bilder aus dem Wohnhaus (von innen und außen), dem Feriendomizil (inklusive Anreise- und Abreisedatum), der Mama (mit Hinweisen zur Freizeitgestaltung) oder der Schwester (inklusive Hinweisen zu Zeiten, wann sich diese wo befindet) gepostet worden wären. Diese Informationen machen ein rein analoges Präventionskonzept zunichte.

Versteckte Social-Media-Hinweise können ein analoges Sicherheitskonzept zunichte machen

Neben der Limitierung der Suchmaschinen für die Suche nach relevanten Informationen im Internet und auf Social-Media-Plattformen ist es vor allem das Know-how und die technische Fähigkeit, auch im Darknet und Deepweb nach Informationen zu suchen. Kriminelle nutzen Peer-to-Peer-Verbindungen, legen Informationen auf „Crime Servern" ab und bieten diese zum Kauf an. Auch kompromittierende Informationen zu Gebäuden, Veranstaltungen, vertraulichen Daten, VIPs, Vorständen oder „Wealthy People" werden dort angeboten. Nur wenn man die Fähigkeit besitzt, auch hier ein 24/7-Radar zu platzieren, kann man von einem umfänglichen Informationsmix sprechen. Es geht nichts ohne die gesunde Mischung aus Tool und Analysten. Neben den digitalen sind es aber vor allem auch die analogen, personenbezogenen Quellen, die von Tätern leicht angezapft werden können. Bleiben wir bei dem erwähnten Beispiel: Nachdem der Täter in Social-Media-Profilen herausgefunden hat, dass Handball das große Hobby des 14-Jährigen ist und sich das Interesse vor allem auf einen Verein konzentriert, ist es ein Leichtes, im Zuge von Social Engineering mehr über die Person, das Umfeld und die Abläufe zu erfahren. Hier ist dann auch die Grenze der Legalität erreicht. Eine direkte Verbindungsaufnahme mit der Schutzperson unter Vorspiegelung falscher Identitäten ist eventuell sogar strafbar. Nicht jedoch Sensibilisierungsmaßnahmen rund um dieses Thema. So wie man früher den Kindern beibrachte, keine Schokolade von Fremden anzunehmen, so muss es heute selbstverständlich sein, auch die digitale Aufmerksamkeit zu schulen.

Fazit

Die Nachfrage zur Sicherheit von Personen im analogen und digitalen Umfeld steigt gerade auch für Unternehmer, die Schutz für sich und ihre Familien suchen. Wenn heute von „Vorfeldaufklärung“ für eine Schutzperson oder eine Veranstaltung gesprochen wird, wähnen sich viele Verantwortliche bereits im Bereich der „Protective Intelligence“. Mitnichten – Der Ansatz geht weit über das Klassische hinaus. Die Nutzung des Quellenmix von Darknet, Deepweb, Social Media, dem Internet bis hin zum Einsatz von Social-Engineering-Techniken muss heute in Betracht gezogen werden. Um die Verfahren zu beherrschen, müssen sowohl Technologien als auch Spezialisten (Analysten) bereitgestellt werden, die in den wenigsten Sicherheitsabteilungen zur Verfügung stehen. Der ausschließliche Einsatz von „Suchmaschinen“ greift zu kurz, da wesentliche Informationen durch Verschleierung von diesen nicht gefunden werden können. „Protective Intelligence“ ist nicht nur personenbezogen. Es kann mannigfaltig eingesetzt werden, um ganzheitlich und kostengünstig Werte zu schützen.

Quellenmix aus Darknet, Deepweb und Social Media zwecks Risikofrüherkennung

BERENBERG
PRIVATBANKIERS SEIT 1590

Literatur:

O. Schneider, www.sicherheit.info/ganzheitlicher-schutz-gefaehrdeter-personen

Sie möchten regelmäßig über die Themen Ihres Kompetenzzentrums informiert werden oder interessieren sich für weitere Publikationen von Berenberg?
Einfach den QR-Code mit Ihrem Smartphone lesen oder anmelden unter: newsletter.berenberg.de

Bei diesem Dokument handelt es sich um eine Marketingmitteilung der Joh. Berenberg, Gossler & Co. KG. Die gemachten Angaben wurden nicht durch eine außenstehende Partei geprüft. Alle Aussagen basieren auf allgemein zugänglichen Quellen. Für die Richtigkeit und Vollständigkeit sämtlicher Angaben übernehmen wir keine Gewähr. Wir weisen ausdrücklich auf den angegebenen Bearbeitungsstand hin. Angaben können sich durch Zeitablauf und/oder infolge gesetzlicher, politischer, wirtschaftlicher oder anderer Änderungen als nicht mehr zutreffend erweisen.
Zur Erklärung verwendeter Fachbegriffe steht Ihnen auf www.berenberg.de/glossar ein Online-Glossar zur Verfügung. Die gewerbliche Nutzung in Form eines Nachdrucks, der – auch teilweisen – Vervielfältigung sowie der Weitergabe des Beitrages ist ohne unsere ausdrückliche schriftliche Genehmigung nicht gestattet.

Joh. Berenberg, Gossler & Co. KG
Neuer Jungfernstieg 20
20354 Hamburg
Telefon +49 40 350 60-0
Telefax +49 40 350 60-900
www.berenberg.de
info@berenberg.de