complexium Agenda - Videokonferenz 25.11.

Personenschutz, Anforderungen und die drei digitalen Ebenen

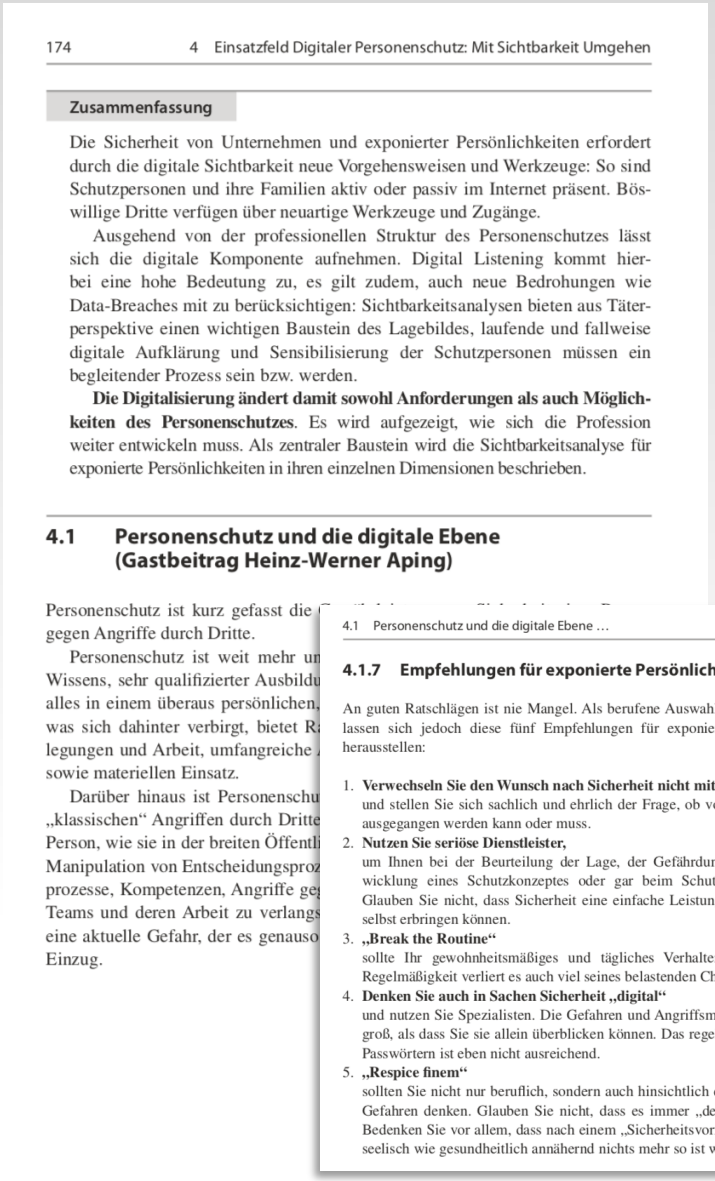
Harte Entscheidungen schaffen Gegner. Böswillige Dritte stoßen im Internet auf Munition und unerwünschte Einblicke. Es entstehen Möglichkeiten der Ansprache und Annäherung.
→ **Gegner müssen nicht mehr mutig sein, Schutzfamilien aber umso achtsamer.**

Wir greifen Anforderungen an den **Personenschutz** mit künftiger, digitaler Relevanz auf. Ein vorausschauendes **Lagebild** muss Bedrohungen aus drei digitalen Ebenen aufnehmen:

- *Publik*: Shitstorms, Kritik und Reputationsangriffe lauern im öffentlichen Raum.
- *Privat:* Einblicke zu Familie, Wohnort, Freizeit und Routinen zielen auf die Privatsphäre.
- *Profil:* Gehackte Nutzerdaten erlauben Ansprachen, ID-Missbrauch, Social Engineering.

Präzise Lagebilder, passender Einsatz von qualifiziertem Personal und eigene Achtsamkeit steigern die Sicherheit der **Schutzfamilien**. Digital Listening leistet einen wichtigen Beitrag.

The Next Line of Defense.



174 4 Einsatzfeld Digitaler Personenschutz: Mit Sichtbarkeit Umgehen

Zusammenfassung

Die Sicherheit von Unternehmen und exponierter Persönlichkeiten erfordert durch die digitale Sichtbarkeit neue Vorgehensweisen und Werkzeuge: So sind Schutzpersonen und ihre Familien aktiv oder passiv im Internet präsent. Böswillige Dritte verfügen über neuartige Werkzeuge und Zugänge.

Ausgehend von der professionellen Struktur des Personenschutzes lässt sich die digitale Komponente aufnehmen. Digital Listening kommt hierbei eine hohe Bedeutung zu, es gilt zudem, auch neue Bedrohungen wie Data-Breaches mit zu berücksichtigen: Sichtbarkeitsanalysen bieten aus Täterperspektive einen wichtigen Baustein des Lagebildes, laufende und fallweise digitale Aufklärung und Sensibilisierung der Schutzpersonen müssen ein begleitender Prozess sein bzw. werden.

Die Digitalisierung ändert damit sowohl Anforderungen als auch Möglichkeiten des Personenschutzes. Es wird aufgezeigt, wie sich die Profession weiter entwickeln muss. Als zentraler Baustein wird die Sichtbarkeitsanalyse für exponierte Persönlichkeiten in ihren einzelnen Dimensionen beschrieben.

4.1 Personenschutz und die digitale Ebene (Gastbeitrag Heinz-Werner Aping)

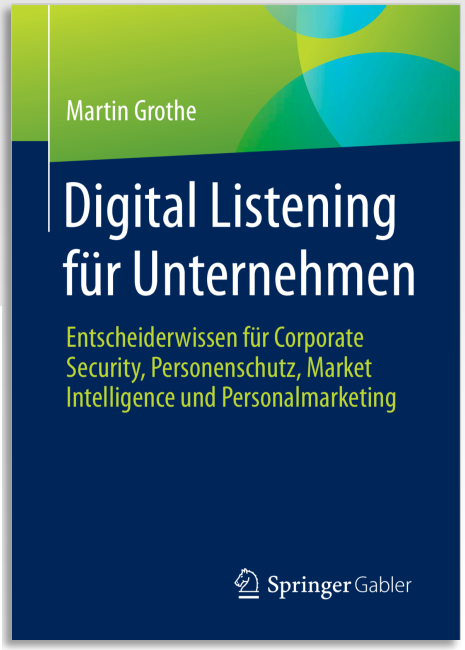
Personenschutz ist kurz gefasst die
gegen Angriffe durch Dritte.
Personenschutz ist weit mehr un
Wissens, sehr qualifizierter Ausbildu
alles in einem überaus persönlichen,
was sich dahinter verbirgt, bietet R
legungen und Arbeit, umfangreiche
sowie materiellen Einsatz.
Darüber hinaus ist Personenschu
„klassischen" Angriffen durch Dritte
Person, wie sie in der breiten Öffentli
Manipulation von Entscheidungsproz
prozesse, Kompetenzen, Angriffe ge
Teams und deren Arbeit zu verlangs
eine aktuelle Gefahr, der es genauso
Einzug.

4.1 Personenschutz und die digitale Ebene … 191

4.1.7 Empfehlungen für exponierte Persönlichkeiten

An guten Ratschlägen ist nie Mangel. Als berufene Auswahl aus vielen Punkten lassen sich jedoch diese fünf Empfehlungen für exponierte Persönlichkeiten herausstellen:

1. **Verwechseln Sie den Wunsch nach Sicherheit nicht mit der Wirklichkeit** und stellen Sie sich sachlich und ehrlich der Frage, ob von einer Gefährdung ausgegangen werden kann oder muss.
2. **Nutzen Sie seriöse Dienstleister,** um Ihnen bei der Beurteilung der Lage, der Gefährdungsanalyse, der Entwicklung eines Schutzkonzeptes oder gar beim Schutz selbst zu helfen. Glauben Sie nicht, dass Sicherheit eine einfache Leistung ist, die Sie immer selbst erbringen können.
3. **„Break the Routine"** sollte Ihr gewohnheitsmäßiges und tägliches Verhalten sein. Über diese Regelmäßigkeit verliert es auch viel seines belastenden Charakters.
4. **Denken Sie auch in Sachen Sicherheit „digital"** und nutzen Sie Spezialisten. Die Gefahren und Angriffsmöglichkeiten sind zu groß, als dass Sie sie allein überblicken können. Das regelmäßige Ändern von Passwörtern ist eben nicht ausreichend.
5. **„Respice finem"** sollten Sie nicht nur beruflich, sondern auch hinsichtlich der Ihnen drohenden Gefahren denken. Glauben Sie nicht, dass es immer „den anderen" passiert. Bedenken Sie vor allem, dass nach einem „Sicherheitsvorfall" in vielen Fällen seelisch wie gesundheitlich annähernd nichts mehr so ist wie zuvor.



Grundlage und Anlass ist das neue Standardwerk „Digital Listening" mit zahlreichen Praxisvertiefungen.
https://www.springer.com/de/book/9783658311032

complexium Agenda - Videokonferenz 25.11.

Personenschutz, Anforderungen und die drei digitalen Ebenen

Wir laden Sie ein, gemeinsam mit uns die notwendige Weiterentwicklung zu diskutieren. Die in Plenum formulierten Empfehlungen werden im Nachgang aufbereitet und geteilt.

Schon vorab interessiert uns Ihre Einschätzung:

1. Sehen Sie besondere Herausforderungen für Personaleinsatz und -qualifikation?
2. Gibt es grundsätzliche Personenschutz-Herausforderungen in Ihrem Umfeld?
3. Welche Erwartung haben Sie an die gemeinsame Runde?

Wir bringen einen engagierten Kreis zusammen und freuen uns über Ihr Interesse.

Lassen Sie uns gemeinsam die Sicherheit exponierter Persönlichkeiten erhöhen.

Videokonferenz

Senden Sie uns Ihr Interesse für die Expertenrunde: agenda@complexium.de

Termin: 25. November 2020, 13:00 – 14:00 Uhr

Teilnehmer: Ausgewählter Expertenkreis mit großem Erfahrungsschatz.

Technik: Bestätigung und Einwahllink zur Videokonferenz werden vorab verschickt.

Prof. Dr. Martin Grothe
grothe@complexium.de

Prof. Dr. Martin Grothe beschäftigt sich seit den 90er Jahren mit der Mustererkennung in komplexen Strukturen: Der Digitalraum entwickelte sich zum perfekten Arbeitsfeld. Martin Grothe gründete nach Stationen im Consulting, Controlling und Community Building in 2004 die complexium GmbH in Berlin.
Als Mission werden mit eigenen Formaten, Methoden und Technologien „Insights" im digitalen Raum strukturiert entdeckt, um Klienten einen Vorsprung in den Bereichen Unternehmenssicherheit, Personenschutz und Market Intelligence zu ermöglichen.
Module der Technologie wurden in Kooperation mit dem Robert-Koch-Institut vom BMBF gefördert: *„Forschung für die zivile Sicherheit".*
Aufbauend entstand etwa mit der Allianz für Sicherheit in der Wirtschaft die Studie: *„#Desinformation: Lage, Prognose und Abwehr."*

Heinz-Werner Aping
aping@complexium.de

Heinz-Werner Aping ist Direktor beim Bundeskriminalamt a. D. und war bis zu seiner Pensionierung 2014 fast vierzig Jahre im kriminalpolizeilichen Dienst in Land und Bund tätig. Als Leitender Kriminaldirektor und Gruppenleiter in der Abteilung Sicherungsgruppe des BKA verantwortete Aping die Bereiche Grundsatz, Haushalt, Ausbildung, Lagebeurteilung, Staatsbesuche, Observation und Technikeinsatz des Personenschutzes für die Verfassungsorgane des Bundes und seiner ausländischen Gäste. Im Jahr 2001 wurde ihm die Leitung der gesamten Abteilung Sicherungsgruppe übertragen, die er bis zu seiner Pensionierung innehatte. Sein Tätigkeitsfeld umfasste neben der Führung der Abteilung im Alltagsgeschäft gleichermaßen den Einsatz als Polizeiführer großer Veranstaltungen wie G 8 oder Nato-Gipfel als auch persönliche Sicherheitsgespräche mit den höchsten politischen Verantwortungsträgern.
Seit 2020 unterstützt er als *„Senior Expert"* auch die Sicherheitslösungen von complexium.