kaspersky

# Geschäftsgeheimnisse im Zug

Ein Kaspersky-Experiment – wie offen gehen wir mit sensiblen Business-Informationen in der Öffentlichkeit um?

Juni/Juli 2019

kaspersky

# Visual und Audible Hacking als unterschätzte Gefahr für Unternehmen

Ob Laptops, Smartphones oder Firmenakten – im Zug gehen wir sehr offen mit Geschäftsgeheimnissen um. Ob aus purer Neugier oder mit krimineller Energie: Oft lesen und hören mehr Menschen mit, als man glauben möchte. Mögliche Folgen für Unternehmen und Organisationen: schwerwiegende Datenschutzverletzungen, Wirtschaftsspionage oder zielgerichtete Cyberattacken. Um die Gefahr des Visual beziehungsweise des Audible Hacking zu verdeutlichen, hat Kaspersky im Rahmen eines Experiments einen Tester damit beauftragt, in von Geschäftsreisenden hochfrequentierten Zügen – anonym und im Schnelldurchlauf per Strichliste – zu analysieren, welche sensiblen Informationen der Business-Welt ohne große Mühen eingesammelt werden können. Die Bilanz nach fünf Tagen und 170 analysierten Waggons: 2.245 potentiell einsehbare und mitzuhörende Informationen wie Name und Unternehmen von Geschäftsleuten beziehungsweise von Kollegen und Partnern. Das entspricht 13 potentiell öffentlich zugänglichen Geschäftsgeheimnissen pro Waggon – wobei in der 1. Klasse mit durchschnittlich 23 pro Abteil die meisten sensiblen Business-Informationen offenbart wurden. Nur auf fünf Prozent der Geschäftslaptops kam eine Sichtschutzfolie zum Einsatz. Sensible Telefongespräche – beispielsweise eines Anwalts – wurden ohne Einschränkung öffentlich im Zug geführt. Vor allem der Einsatz geschäftlicher E-Mails – mit 58 Prozent das am häufigsten im Zug verwendete Business-Programm – offenbart Dritten frei Haus sensible Unternehmensinformationen, die in der Öffentlichkeit nichts verloren haben.

**Ausgangslage:** Mit zunehmender WLAN-Abdeckung sowie der weiten Verbreitung von Geschäftshandys und -Laptops steigt die Gefahr, dass Mitarbeiter eines Unternehmens im öffentlichen Raum Geschäftsgeheimnisse preisgeben, ohne es wirklich zu bemerken.

Ein gutes Beispiel hierfür sind Geschäftsreisende im Zug. Denn seit die Deutsche Bahn kostenfreies WLAN anbietet, ist es einfach wie nie, während der Fahrt E-Mails, Präsentationen oder sonstige Dokumente zu bearbeiten. Auch das Smartphone wird für Abstimmungen mit Geschäftspartnern, Kunden oder Kollegen in der Öffentlichkeit häufig ohne Bedenken gezückt.

Allerdings ist das Zugabteil nicht das eigene Büro. Geschäftliche Informationen – ob auf dem Laptop einsehbar oder über ein Telefonat mitzuhören – sind nicht für die Mitreisenden bestimmt. Sie sollten auch während einer Geschäftsreise vertraulich behandelt werden. Ansonsten läuft man Gefahr, visuell oder auditiv gehackt zu werden.

Doch sind sich die E-Mail-Schreiber und Vieltelefonierer im Zug dessen wirklich bewusst? Riskieren sie die Reputation der eigenen Firma – und liefern unfreiwillig Futter für einen zielgerichteten Angriff oder Industriespionage? Sollten Unternehmen ihre Mitarbeiter verstärkt in puncto Sicherheitsverhalten auf Geschäftsreisen schulen – gerade im Hinblick auf die DSGVO?

Visual Hacking als unterschätzte Gefahr für Unternehmen (Quelle shutterstock 218159434)

**Aufbau des Experiments:** Kaspersky beauftragte für das Experiment einen Tester, der zwischen Ostern und Pfingsten 2019 fünf Tage lang auf bei Geschäftsreisenden beliebten Zugstrecken in Deutschland unterwegs war, um die Gefahr für Unternehmen von Visual beziehungsweise Audible Hacking auszuloten. Dabei wurden die Passagiere nicht ausspioniert! Der Tester hat lediglich die offenen Geschäftsgeheimnisse, die ihm im Zug begegneten anhand einer Strichliste gezählt und kategorisiert – vollkommen anonym. Zudem wurden – sofern der Anschaulichkeit des Experiments zuträglich – ein paar Anekdoten (ebenfalls vollkommen anonym) notiert. Die Erhebungsbasisdaten und der Fragebogen können bei Berkeley Kommunikation (kaspersky_de@berkeleypr.com) angefordert werden.

**Ziel des Experiments** ist es, auf das zu nachlässige Verhalten von Geschäftsreisenden sowie der Gefahr des Audible/Visual Hacking aufmerksam zu machen. Denn: Was hilft der beste mobile Virenschutz, wenn bestimmte Informationen öffentlich sichtbar gemacht oder hörbar werden. Es geht nicht darum, eine Person detailliert auszuspionieren beziehungsweise um Hacking-Attacken über unsichere WLAN-Netze oder Bluetooth-Verbindungen; es soll illustriert werden, wie viele vertrauliche Geschäftsinformationen im Zug aufgrund nachlässigen Verhaltens für Jedermann ersichtlich und vernehmlich kursieren – und so zur häufig unterschätzten Gefahr für Unternehmen werden können. Denn eines hat das Kaspersky-Experiment gezeigt: Züge in Deutschland sind ein wahres Schlaraffenland für Visual und Audible Hacker.

**Der Tester:** Als Experte für Personalmarketing-Konzepte und Produzent der Web-Serie JobSHAKER TV legt Stephan Schilling im Jahr weit mehr als 120.000 Kilometer per Bahn in Deutschland zurück. Er kennt die Herausforderungen, die sich stellen, wenn man unterwegs arbeiten muss und gleichzeitig den Datenschutz im Blick behalten sollte.

kaspersky

## Methodik

Die Basisfrage des Experiments lautete: Gefahr durch Visual und Audible Hacking – wie viele Menschen geben im Zug unbewusst Geschäftsinformationen preis, via Papier-Dokumente, Bildschirme und/oder Telefonate?

Verhaltensrahmen für den Tester: Der Tester hat seine Auswertung pro Zugwagen durchgeführt. Dabei hat er das jeweilige Abteil durchschritten (zweimal) und abhängig von der Auslastung zwischen zwei und sechs Minuten im Waggon für seine Analyse verbracht. War ein Sitzplatz frei, hat er diesen eingenommen, um sich einen Überblick über die Situation verschaffen zu können. War kein Sitzplatz frei, hat er sich im Gang aufgehalten, um seine Messung durchzuführen. Der Tester hat also sowohl im Sitzen als auch im Vorbeigehen seine Strichliste geführt. Wobei er die meisten Zählungen – gerade bei den Displays – im Vorbeigehen gemacht wurden, was wiederum zeigt, wie virulent die Gefahr ist, dass Dritte im Vorbeigehen eine womöglich sensible Geschäftsinformation aufschnappen könnten. Wichtige Vorgabe: Der Tester durfte nicht als Tester auffallen, damit die Untersuchungssituation im Zug unverändert blieb.

Die Werte wurden über eine Strichliste erhoben und anschließend über eine Häufigkeitstabelle ausgewertet. Es handelt sich hierbei um eine Stichprobe: Die ermittelten Werte sind nicht repräsentativ. Sie sollen die Häufigkeit von im Zug öffentlich arbeitenden Menschen lediglich illustrieren. Die hier ermittelten Werte sind exemplarisch zu sehen.

Der Test: Zwischen Ostern und Pfingsten war der Tester fünf Tage lang auf hoch frequentierten Bahnstrecken unterwegs, um die Zählung durchzuführen. Die Testtage waren unter der Woche und nicht in den Ferien, um einen hohen Anteil an Geschäftsreisenden gewährleisten zu können. Zudem wurden bei Geschäftsreisenden beliebte Strecken wie Berlin-München, Köln-Frankfurt, Berlin-Hamburg sowie Berlin-Hannover-Köln getestet.

Insgesamt wurden 170 Zugwägen inspiziert. Davon 110 aus der 2. und 43 aus der 1. Klasse. Hinzu kommen noch 17 Bistrowägen.

Neben qualitativen Erkenntnissen wurden quantitativ die folgenden Merkmale als Strichliste erfasst:

1. Physische Geschäftsdokumente

2. Ersichtliche Bildschirme von Geschäftsreisenden

3. Geschäftstelefonate

4. WLAN-Verbindungen

## Die Ergebnisse

Neben der Strichlistenzählung sensibler Informationen im Geschäftsumfeld erlebte der Tester aus datenschutztechnischer Sicht einige bemerkenswerte Situationen.

Worst-Case-Anekdoten:

• Ein Reisender verwendete einen Laptop, der mit einer ID-Card gesichert war oder eine Verbindung genutzt hat, die eine solche ID-Card benötigt – zur 2-Faktor-Authentifizierung. Auf der ID-Card waren allerdings Klarname, Unternehmen und eine ID-Nummer eindeutig zu erkennen. Ein Beispiel dafür, wie selbst eine Sicherheitsmaßnahme Informationen verrät, die nicht in die Öffentlichkeit gehören.

• Ein Reisender (vermutlich Anwalt) führte ein langes Telefongespräch über einen juristischen Fall. Darin wurden Klarnamen der Verfahrensbeteiligten, das Prozess führende Gericht sowie Details des Falles sehr laut besprochen.

• Ein Professor bearbeitet Klausuren/Abschlussarbeiten von Studenten. Matrikelnummern und Namen der Studenten waren sichtbar.

Lobenswert:

• Eine mutmaßliche Beraterin führte ein 20-minütiges Telefongespräch, ohne einen Unternehmensnamen, Klarnamen oder sonstige identifizierbare Daten zu verwenden. Es wurden Codewörter benutzt oder Dinge und Sachverhalte so umschrieben, dass sie für Nicht-Beteiligte nicht identifizierbar oder verständlich waren.

***Das Urteil des Testers***

*„Das Kaspersky-Experiment hat mir meine bisherige Vermutung, dass Geschäftsreisende oft zu sorglos mit Unternehmensinformationen umgehen, definitiv bestätigt. Die Reisenden haben oft kein Bewusstsein dafür, dass Visual und Audible Hacking ein riesiges Datenschutzproblem darstellen*

*„Die WLAN-Abdeckung und Zuverlässigkeit in der Deutschen Bahn hat sich im Vergleich zu früheren Zeiten stark verbessert. Ein Grund dafür, dass ich beim Kaspersky-Experiment keine unsicheren WLAN-Netze entdecken konnte. Allerdings steigt die Tendenz, dank guter WLAN-Verbindung im Zug, das Internet in aller Öffentlichkeit für berufliche Zwecke zu nutzen. Die Nutzungshürde ist heute einfach sehr gering – ein Häkchen auf dem angebotenen DB-WLAN-Netz setzen und man kann im Zug surfen.“*

*„Vor allem die Nutzung von E-Mail gibt freien Blick auf Unternehmensdaten. Allein durch Signatur und Betreff werden für Dritte geschäftliche Geheimnisse offenbart, die in der Öffentlichkeit nichts zu suchen haben.“*

*„Ob privat oder beruflich – wir müssen lernen, dass nicht nur unsere Spuren im Web nachverfolgt werden können, sondern dass wir häufig – ohne es zu merken – über digitale Geräte direkten Einblick in persönliche und geschäftliche Geheimnisse gewähren. Gerade für Firmen ist das meiner Meinung nach ein riesiges Datenschutzproblem.“*

*„Der digitale Wandel verstärkt Visual und Audible Hacking. Warum? Weil es mittlerweile egal ist, wo und wann wir arbeiten. Ob im Zug, am Flughafen oder im Café – sensible Unternehmensinformationen müssen an anderen Orten ebenso geschützt werden wie im Büro. Das bedeutet allerdings, dass wir uns der Gefahr bewusst werden sowie passende Sicherheitsmaßnahmen wie den Einsatz von Sichtschutzfolie ergreifen müssen.“*

*„Mein Tipp an mitreisende Geschäftsleute: Bevor man beispielsweise ein Telefonat im Zug führt, sollte man sich immer fragen, ob das wirklich genau jetzt sein muss. Wenn ja, muss man sich immer bewusst machen, dass alle anderen in der Umgebung mithören – ob gewollt oder ungewollt. Also sparsam mit Namen und sensiblen Informationen umgehen.“*

## Physische Dokumente wie Akten

Insgesamt wurden laut der Kaspersky-Stichprobe 281 berufliche Dokumente bearbeitet – 24 Fahrgäste haben ein Dokument aktiv verfasst und 257 haben es gelesen. Insgesamt waren 160 Klarnamen ersichtlich – beispielsweise des Reisenden oder seines Unternehmens.

Der Grund: Zahlreiche Geschäftsreisende hatten Ausdrucke (oft von Vorträgen oder Präsentationen) oder Formulare (wie Reisekostenabrechnungen) dabei, bei denen Logo, Kopf- und Fußzeile für die Mitreisenden ein Fundus an geschäftlichen Informationen darboten.

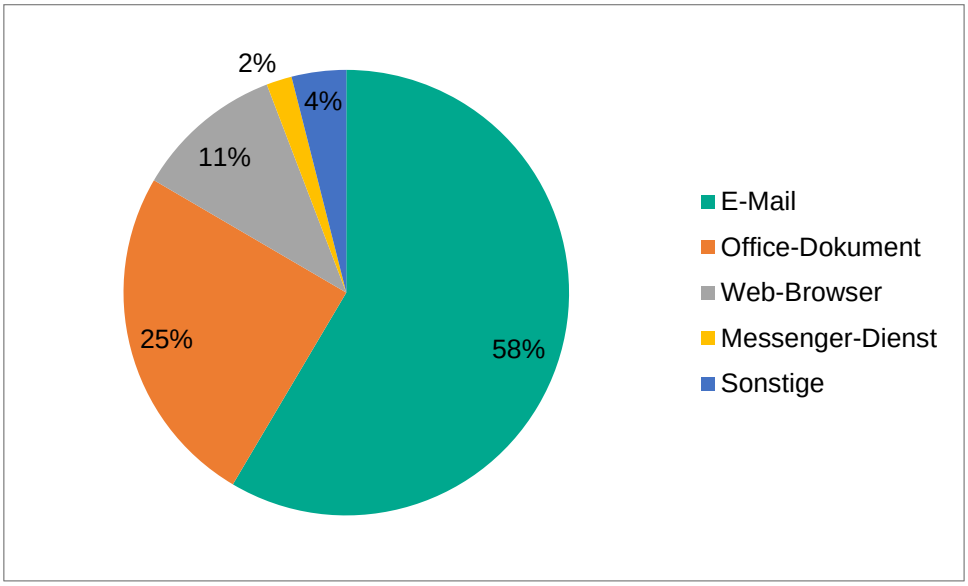
Visual-Hacking-Gefahr: Laptopbildschirme mit geschäftlichen Inhalten

## Bildschirme von Laptops und Co.

Auf 1.193 Bildschirmen wurde für den Tester offensichtlich ein Business-Programm genutzt. Davon 1.041 auf einem Laptop, 69 auf einem Smartphone und 83 auf einem Tablet. Lediglich bei fünf Prozent der Laptops (49 Stück) wurde eine Sichtschutzfolie verwendet.

Analysiert man, welche Programme auf allen 1.193 Bildschirmen für den Tester offensichtlich genutzt wurden, ergibt sich folgendes Bild:

- E-Mail: 699 (58 Prozent)
- Office-Dokument: 297 (25 Prozent)
- Web-Browser: 128 (11 Prozent)
- Messenger-Dienst: 22 (2 Prozent)
- Sonstiges: 47 (4 Prozent)




Anteil der über Bildschirme (1.193 Stück) genutzten Geschäftsprogramme im Zug

E-Mails machen mit 58 Prozent der im Zug genutzten Business-Programme den Löwenanteil aus. Das Datenschutzproblem: E-Mails verraten Details über die Signatur, den Betreff oder den Empfänger. Gerade wenn sie – wie im Experiment bestätigt – auf Laptopbildschirmen dargestellt sind. Diese Problematik ist bei Smartphones aufgrund des kleineren Bildschirms etwas geringer. Allerdings konnte der Kaspersky-Tester feststellen, dass Geschäftsleute bei der Bearbeitung ihrer E-Mails auf dem Smartphone ihre Programme entsprechend vergrößern und somit die Sichtbarkeit auch für andere erhöhen.

In 960 Fällen konnte der Tester inhaltliche Details einsehen, die sich wie folgt kategorisieren lassen:

• Klarnamen des Unternehmens des Geschäftsreisenden: 842

• Klarnamen des Geschäftsreisenden: 677

• Klarnamen von Kunden- oder Partnerunternehmen: 231

• Klarnamen eines Kunden, Partners, Kollegen: 131

## Geschäftstelefonate

Geschäftstelefonate, die mit einem Abstand von etwa zwei Metern für den Tester hörbar waren: 106 – mit den folgenden Details:

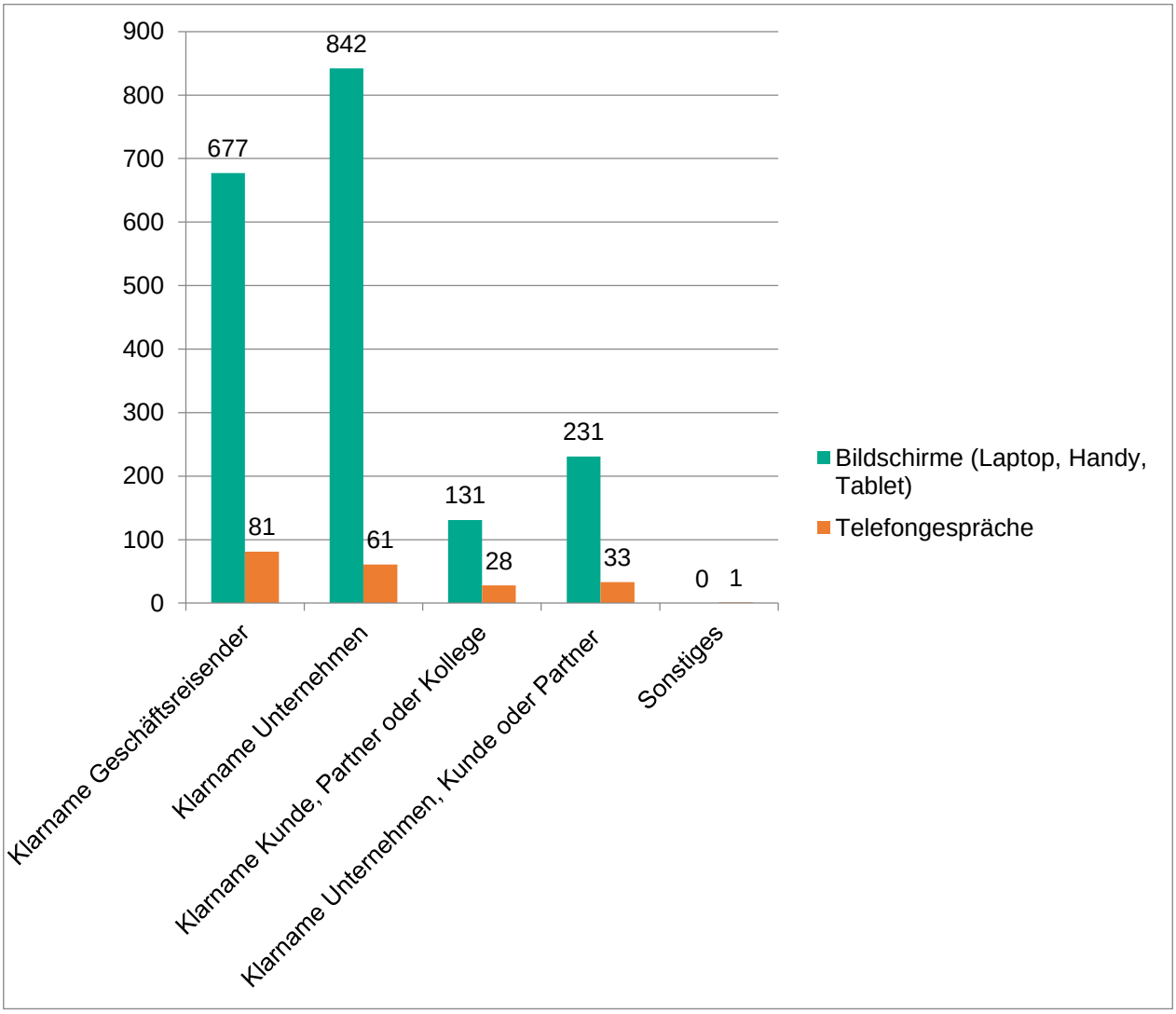
• Klarnamen des Geschäftsreisenden: 81

• Klarnamen des Unternehmens des Geschäftsreisenden: 61

• Klarnamen eines Kunden- oder Partnerunternehmens: 33

• Klarnamen eines Kunden, Partners oder Kollegen: 28

• Sonstiges: 1

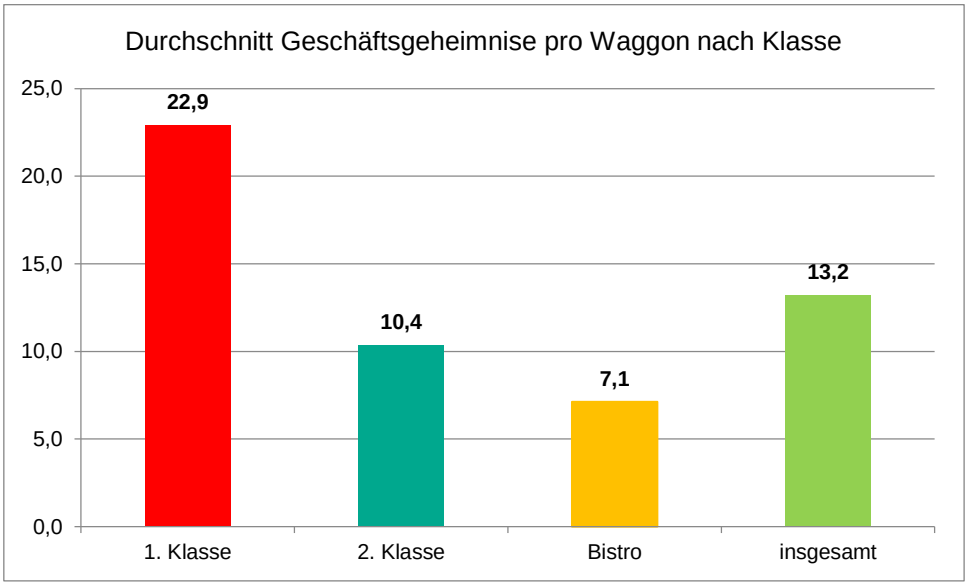



Anzahl und Art der vom Tester notierter Geschäftsinformationen

## Zusammenfassung Dokumente, Bildschirme und Telefonate

Während des Kaspersky-Experiments konnte der Tester 281 physische Dokumente und 1.193 Bildschirme mit Business-Bezug anonym und nur per Strichlistenzählung einsehen. Hinzu kommen 106 mithörbare Geschäftstelefonate.

Dabei wären potentiell **2.245 Geschäftsgeheimnisse** wie Name und Unternehmen der Geschäftsreisenden selber sowie von Kollegen, Kunden und Partner für die anderen Zuggäste zu erspähen beziehungsweise mitzuhören gewesen – und das an nur fünf Testtagen und exemplarischen Routen mit insgesamt 170 Wägen. Das heißt: **13 sensible Geschäftsinformationen pro Waggon** waren während des Experiments öffentlich zugänglich. Dieses Beispiel illustriert, wie hoch die potentielle Menge der in der Bahn herumschwirrenden Geschäftsinformationen ist. Interessant: Durchschnittlich waren in der 1. Klasse 23, in der 2. Klasse zehn und im Bistro sieben Business-Informationen zugänglich (siehe nachfolgende Grafik).




Die meisten potentiell sensiblen Business-Informationen geben Geschäftsreisende der 1. Klasse preis – mit durchschnittlich 23 signifikant mehr als im Durchschnitt (13) und in der 2. Klasse (10)

Laut der Kaspersky-Zählung (siehe folgende Tabelle) waren auf der Strecke Frankfurt-Leipzig besonders viele Geschäftsgeheimnisse auf Bildschirmen zu sehen – 222 insgesamt während einer Fahrdauer von drei Stunden in 12 Waggons (18.5 im Durchschnitt). Allerdings sind für das Aufkommen potentiell öffentlicher Geheimnisse die Strecke, der Tag und die Uhrzeit wichtige Faktoren, die im Rahmen des Experiments auf allen Strecken unterschiedlich waren. Dennoch vermittelt die Häufigkeit von im Zug abgreifbaren Business-Informationen die Gefahr böswilliger Folgeaktionen gegen Unternehmen und Mitarbeiter.

Am meisten verraten Mitarbeiter über ihr Unternehmen aufgrund ihres zu sorglosen Umgangs mit Laptops, Smartphones und Tablets. Sie geben einen verräterischen Einblick in die Büros und Meetingräume von Organisationen. Auch Telefongespräche sollten nicht unterschätzt werden; denn schnappt ein Dritter eine für ihn interessante Information auf, könnte das eine genauere Beschäftigung damit nach sich ziehen.

| | | | | DOKUMENTE | | BILDSCHIRME | | TELEFONATE | |
|---|---|---|---|---|---|---|---|---|---|
| Zug | Startbahnhof | Zielbahnhof | Abfahrt und Ankunft | Anzahl Dokumente | Anzahl Geschäftsgeheimnisse | Anzahl Business-Programme | Anzahl Geschäftsgeheimnisse | Anzahl Telefonate | Anzahl Geschäftsgeheimnisse |
| ICE 625 | Essen Hbf | Frankfurt(Main) Hbf | 05/06/2019 10:41 - 12:48 | 15 | 13 | 53 | 125 | 8 | 20 |
| ICE 625 | Frankfurt (Main) Hbf | Aschaffenburg | 05/06/2019 12:54 - 13:22 | 10 | 4 | 79 | 178 | 7 | 15 |
| ICE 576 | Frankfurt (Main) Hbf | Hannover Hbf | 05/06/2019 14:58 - 17:17 | 32 | 25 | 123 | 212 | 9 | 22 |
| ICE 576 | Hannover Hbf | Hamburg Hbf | 05/06/2019 17:20 - 18:35 | 17 | 10 | 63 | 95 | 7 | 13 |
| *Fahrtdauer: 7.95 Stunden / 36 analysierte Zugwaggons* | | | | **74** | **52** | **318** | **610** | **31** | **70** |
| ICE 941 | Essen Hbf | Hannover Hbf | 04/06/2019 14:23 - 16:28 | 11 | 10 | 56 | 90 | 4 | 5 |
| ICE 1681 | Hannover Hbf | Göttingen | 04/06/2019 16:26 - 17:01 | 6 | 4 | 25 | 31 | 3 | 7 |
| ICE 786 | Göttingen | Hannover Hbf | 04/06/2019 17:55 - 18:32 | 8 | 5 | 41 | 56 | 2 | 5 |
| ICE 844 | Hannover Hbf | Essen Hbf | 04/06/2019 19:31 - 21:34 | 10 | 6 | 60 | 108 | 5 | 9 |
| *Fahrtdauer: 7.11 Stunden / 29 analysierte Zugwaggons* | | | | **35** | **25** | **182** | **285** | **14** | **26** |
| ICE 1558 | Dresden Hbf | Leipzig Hbf | 15/05/2019 12:10 - 13:24 | 1 | 1 | 23 | 22 | 1 | 3 |
| ICE 508 | Leipzig Hbf | Berlin Hbf | 15/05/2019 14:10 - 15:29 | 6 | 1 | 47 | 60 | 3 | 7 |
| ICE 508 | Berlin Hbf | Hamburg Hbf | 15/05/2019 15:40 - 17:24 | 18 | 6 | 107 | 171 | 6 | 10 |
| *Fahrtdauer: 5.14 Stunden / 22 analysierte Zugwaggons* | | | | **25** | **8** | **177** | **253** | **10** | **20** |
| ICE 1109 | Köln Hbf | Frankfurt(Main) | 14/05/2019 13:55 - 14:50 | 61 | 32 | 137 | 185 | 21 | 34 |
| ICE 596 | Frankfurt (Main) Hbf | Leipzig Hbf | 14/05/2019 16:08 - 19:10 | 35 | 13 | 151 | 222 | 8 | 10 |
| ICE 1655 | Leipzig Hbf | Dresden Hbf | 14/05/2019 20:31 - 21:38 | 7 | 3 | 20 | 34 | 0 | 0 |
| *Fahrtdauer: 7.38 Stunden / 29 analysierte Zugwaggons* | | | | **103** | **48** | **308** | **441** | **29** | **44** |
| ICE 1028 | Köln Hbf | Hamburg Hbf | 13/05/2019 04:00 - 08:33 | 4 | 3 | 30 | 36 | 0 | 0 |
| ICE 599 | Hamburg Hbf | Berlin Hbf | 13/05/2019 09:35 - 11:22 | 14 | 8 | 74 | 115 | 7 | 15 |
| ICE 509 | Berlin Hbf | München Hbf | 13/05/2019 12:30 - 17:01 | 12 | 10 | 39 | 61 | 8 | 19 |
| ICE 590 | München Hbf | Mannheim Hbf | 13/05/2019 18:28 - 21:29 | 10 | 5 | 37 | 42 | 5 | 8 |
| ICE 100 | Mannheim Hbf | Köln Hbf | 13/05/2019 21:35 - 23:08 | 4 | 1 | 28 | 38 | 2 | 2 |
| *Fahrtdauer: 19.08 Stunden / 54 analysierte Zugwaggons* | | | | **44** | **27** | **208** | **292** | **22** | **44** |
| | | | **gesamt** | **281** | **160** | **1193** | **1881** | **106** | **204** |
| | | | | ***Fahrtdauer: 46.66 Stunden / 170 analysierte Zugwaggons*** | | | | | |

Tabelle der über Dokumente, Bildschirme und Telefonate unfreiwillig gegebenen Geschäftsinformationen. In rot, besonders hohes Aufkommen von Business-Informationen. Insgesamt wurden 170 Waggons in über 46 Stunden vom Kaspersky-Tester inspiziert

## Externe WLAN-Nutzung

Positiv: Der Tester konnte keine ungeschützten WLAN-Verbindungen ausfindig machen. Die 37 identifizierten Spots waren geschützt. Aufgrund der mittlerweile guten WLAN-Abdeckung in ICE-Zügen der Deutschen Bahn verzichten die Fahrgäste auf eigene mobile Hotspots und damit auf unsichere Verbindungen. Eine weiteres Ergebnis: Der persönliche Name in SSID (Service Set Identifier: Hinter der Bezeichnung versteckt sich der Name einzelner WLAN-Netzwerke) war in 10 Fällen ersichtlich – was aber kein Grund für Sicherheitsbedenken ist.

Audible Hacking sollte nicht unterschätzt werden (Quelle shutterstock 1028057065)

# Kaspersky-Tipps –Visual und Audible Hacks vorbeugen

Das Kaspersky-Experiment zeigt: Nachlässigkeit mit für andere Zugreisende ersichtlichen Dokumenten und Programmen sowie über Gespräche und Telefonate mithörbare Informationen können empfindliche DSGVO-Verletzungen darstellen – und zwar mit Low-Tech-Methoden.

Auch Wirtschaftsspionage und zielgerichtete Cyberattacken könnten negative Folgen allzu offensichtlicher, für die Öffentlichkeit zugänglicher Geschäftsinformationen sein. Denn sowohl geschäftliche (Name der Firma und/oder des Mitarbeiters, Mailadressen, Produktinformationen etc.) als auch private (Lieblingsfilm, präferierter Fußballverein etc.) Informationen befeuern die Gefahr eines gezielten Angriffs. Spear-Phishing und Waterhole-Angriffe [1] – meist über E-Mails – sind nach wie vor das größte Einfallstor für Cyberangreifer. Je mehr über ein Opfer oder die anvisierte Organisation bekannt ist, desto höher ist die Wahrscheinlichkeit, dass ein Mitarbeiter oder eine Privatperson in einer vertrauenserweckenden, weil personalisierten E-Mail, auf einen gefährlichen Link oder einen kompromittierten Anhang klickt.

Kaspersky Lab empfiehlt Mitarbeitern und Unternehmen die folgenden Sicherheitstipps, um nicht Opfer von Visual beziehungsweise Audible Hacking zu werden:

• Blickschutzfilter oder Blickschutzbildschirme verwenden – die optische Hürde lässt unliebsamen Spähern wenig Chance.

• Sollte keine Sichtschutzfolie vorhanden sein, einen Platz wählen, der Dritten keinen Einblick in Geschäftsprogramme und -informationen gewährt.

• Nur Dinge bearbeiten, die unverfänglich sind; zum Beispiel eine nicht vertrauliche Power-Point-Präsentation. Sensible Aktionen – wie eine E-Mail über ein zum Beispiel noch nicht veröffentlichtes Produkt – gehören in eine sichere Umgebung – und nicht in den Zug.

• Bei Telefonaten immer daran denken, dass das komplette Zugabteil zwangsläufig mithört. Die Nennung von Klarnamen (des Unternehmens, von Kunden oder sonstigen Partnern) vermeiden.

• Geräte nie aus dem Auge lassen; ist dennoch der Gang auf die Toilette nötig, sollten die Geräte entsprechend gesperrt sein (PIN, Zugangsberechtigung oder Passwort) sowie mit einer passenden mobilen Sicherheitslösung [2] ausgestattet sein. Token, ID-Karten oder ähnliches sollten abgezogen und mitgenommen werden.

• Das Verhalten der Mitarbeiter in puncto IT-Sicherheit und Datenschutz auf Geschäftsreisen in den Sicherheitsrichtlinien des Unternehmens festlegen und Empfehlungen aussprechen.

• Mitarbeiter regelmäßig über Cybergefahren und Datenschutz schulen – insbesondere was auf Geschäftsreisenden zu beachten ist. Kaspersky bietet für alle Unternehmensgrößen und Mitarbeiterprofile passende Trainings [3].

• Logos haben auf Geschäftslaptops nichts zu suchen. Auch auf den Inventar-Aufklebern sollten nur Nummern oder Barcodes angebracht werden.

[1] https://www.kaspersky.de/resource-center/definitions/spear-phishing

[2] https://www.kaspersky.de/small-to-medium-business-security/endpoint-select

[3] https://www.kaspersky.de/enterprise-security/security-awareness

www.kaspersky.com/
www.securelist.com