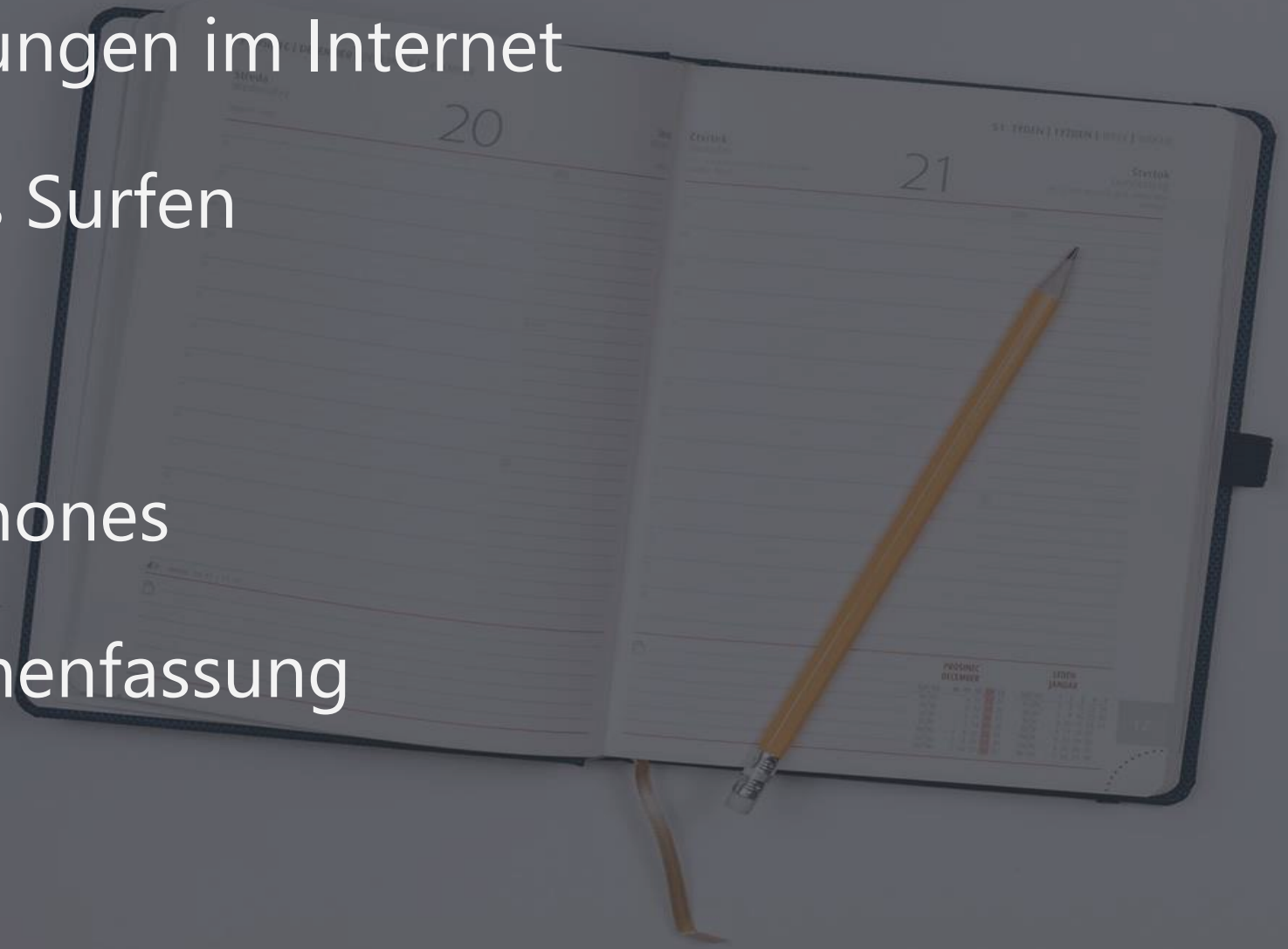
# Sichere Kommunikation im Internet

## Tipps für die Praxis


18.11.2021 Autor: Jonas Grasediek

# Agenda

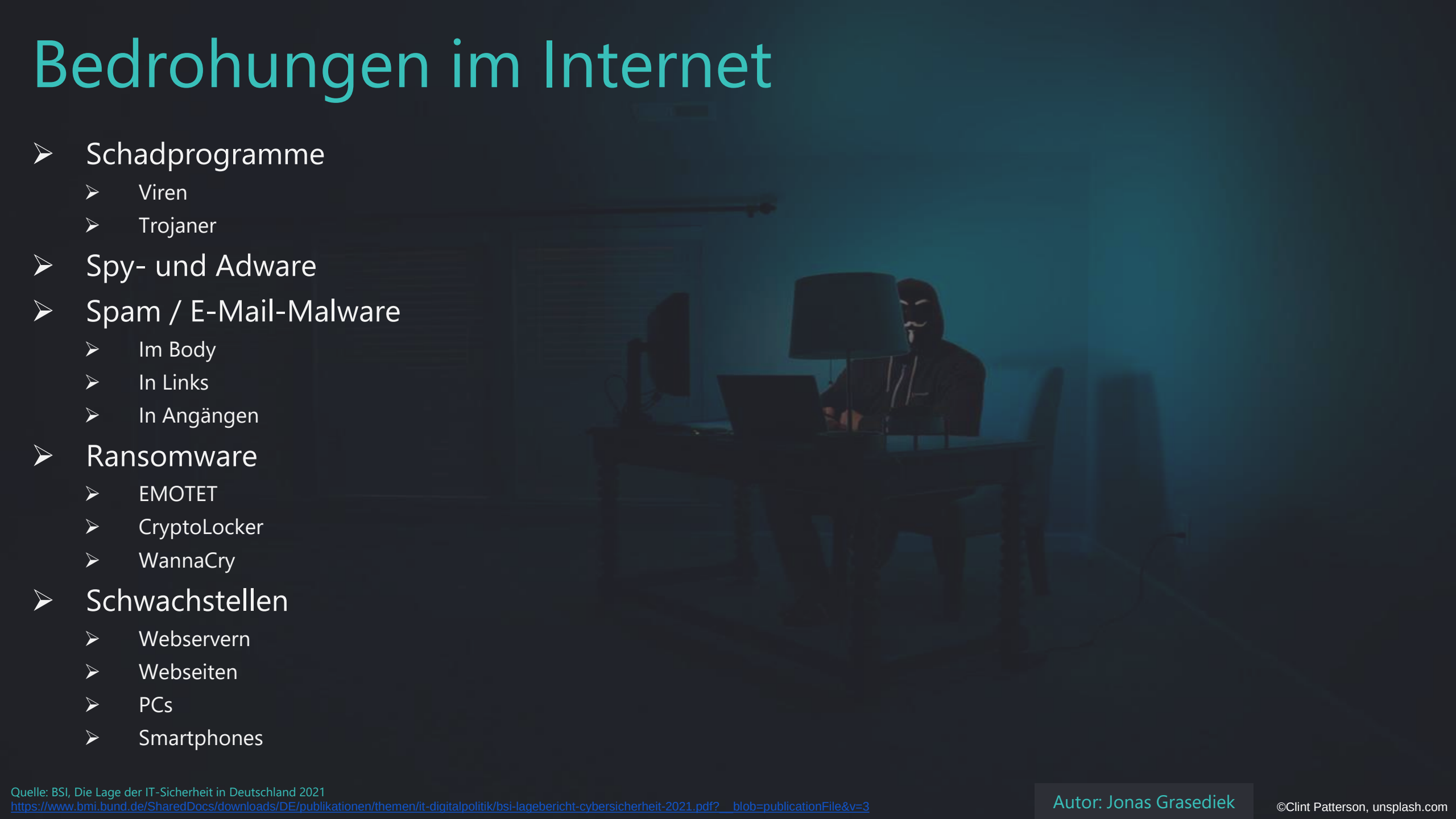
- Bedrohungen im Internet
- Sicheres Surfen
- E-Mails
- Smartphones
- Zusammenfassung



Autor: Jonas Grasediek

# Bedrohungen im Internet

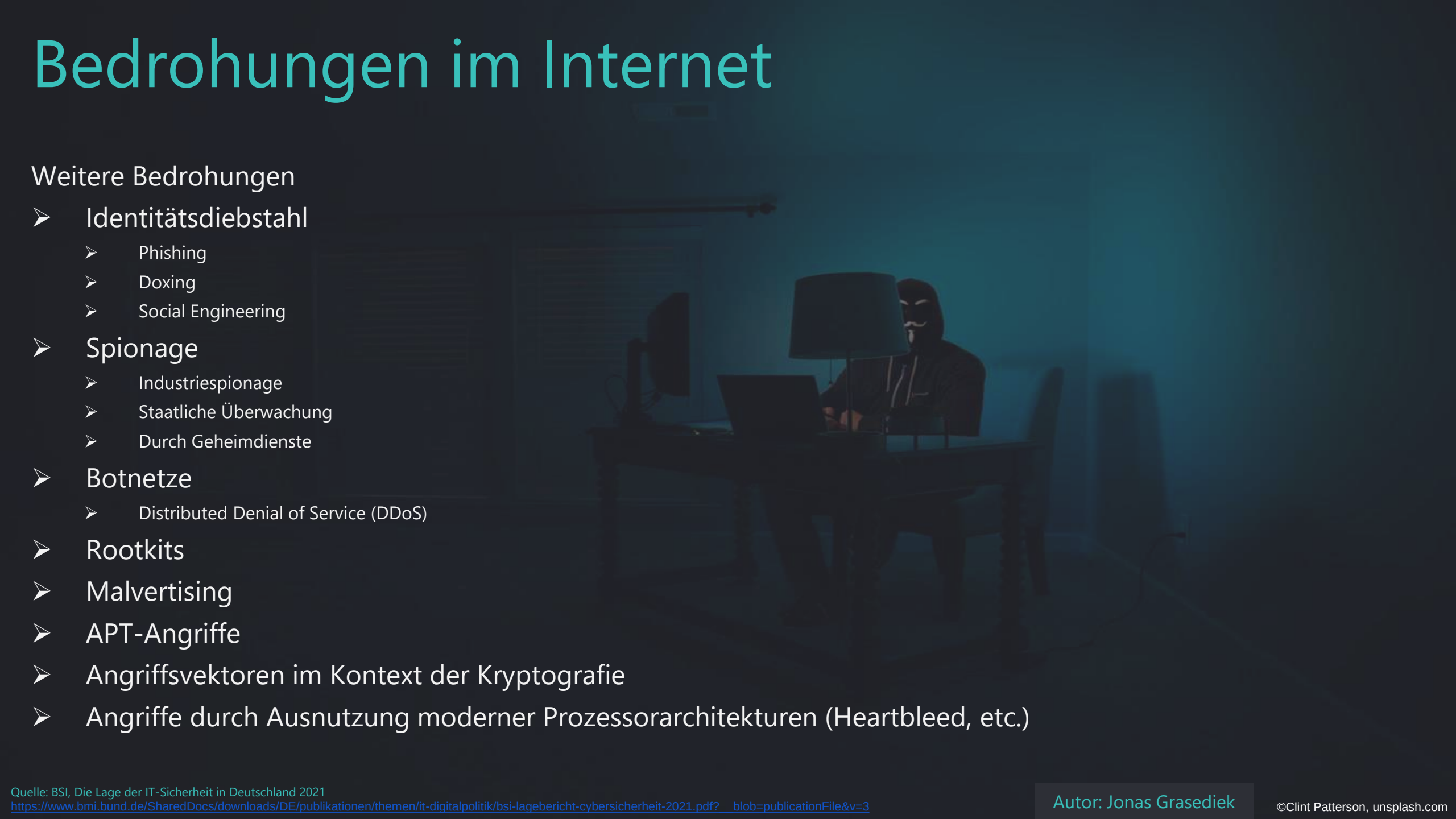
- Schadprogramme
  - Viren
  - Trojaner
- Spy- und Adware
- Spam / E-Mail-Malware
  - Im Body
  - In Links
  - In Angängen
- Ransomware
  - EMOTET
  - CryptoLocker
  - WannaCry
- Schwachstellen
  - Webservern
  - Webseiten
  - PCs
  - Smartphones



Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2021
https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3

Autor: Jonas Grasediek

# Bedrohungen im Internet



Weitere Bedrohungen

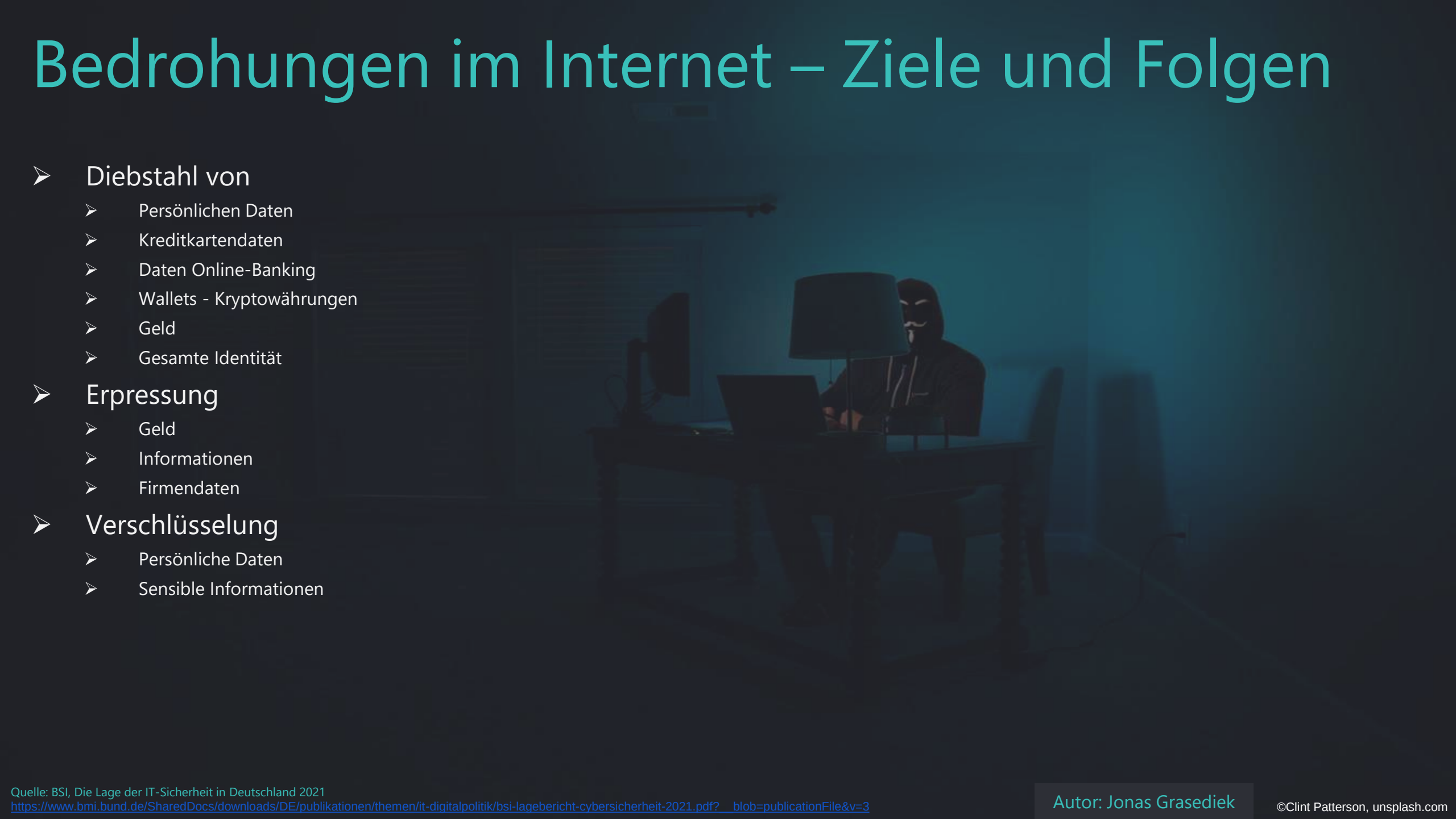
- Identitätsdiebstahl
  - Phishing
  - Doxing
  - Social Engineering
- Spionage
  - Industriespionage
  - Staatliche Überwachung
  - Durch Geheimdienste
- Botnetze
  - Distributed Denial of Service (DDoS)
- Rootkits
- Malvertising
- APT-Angriffe
- Angriffsvektoren im Kontext der Kryptografie
- Angriffe durch Ausnutzung moderner Prozessorarchitekturen (Heartbleed, etc.)

Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2021
https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3

Autor: Jonas Grasediek

# Bedrohungen im Internet – Ziele und Folgen

- Diebstahl von
  - Persönlichen Daten
  - Kreditkartendaten
  - Daten Online-Banking
  - Wallets - Kryptowährungen
  - Geld
  - Gesamte Identität
- Erpressung
  - Geld
  - Informationen
  - Firmendaten
- Verschlüsselung
  - Persönliche Daten
  - Sensible Informationen

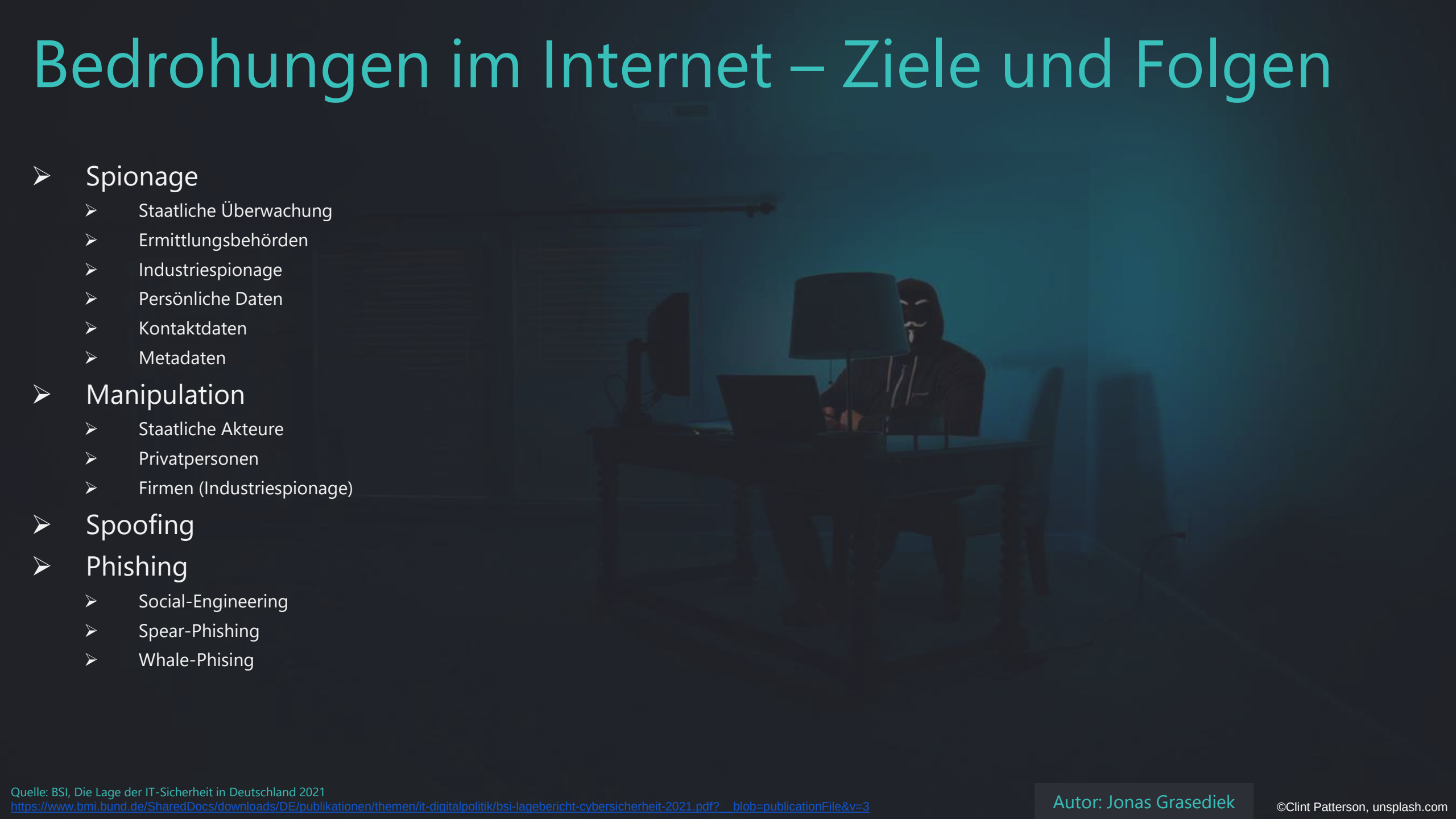


Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2021
https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3

Autor: Jonas Grasediek

# Bedrohungen im Internet – Ziele und Folgen

- Spionage
  - Staatliche Überwachung
  - Ermittlungsbehörden
  - Industriespionage
  - Persönliche Daten
  - Kontaktdaten
  - Metadaten
- Manipulation
  - Staatliche Akteure
  - Privatpersonen
  - Firmen (Industriespionage)
- Spoofing
- Phishing
  - Social-Engineering
  - Spear-Phishing
  - Whale-Phising

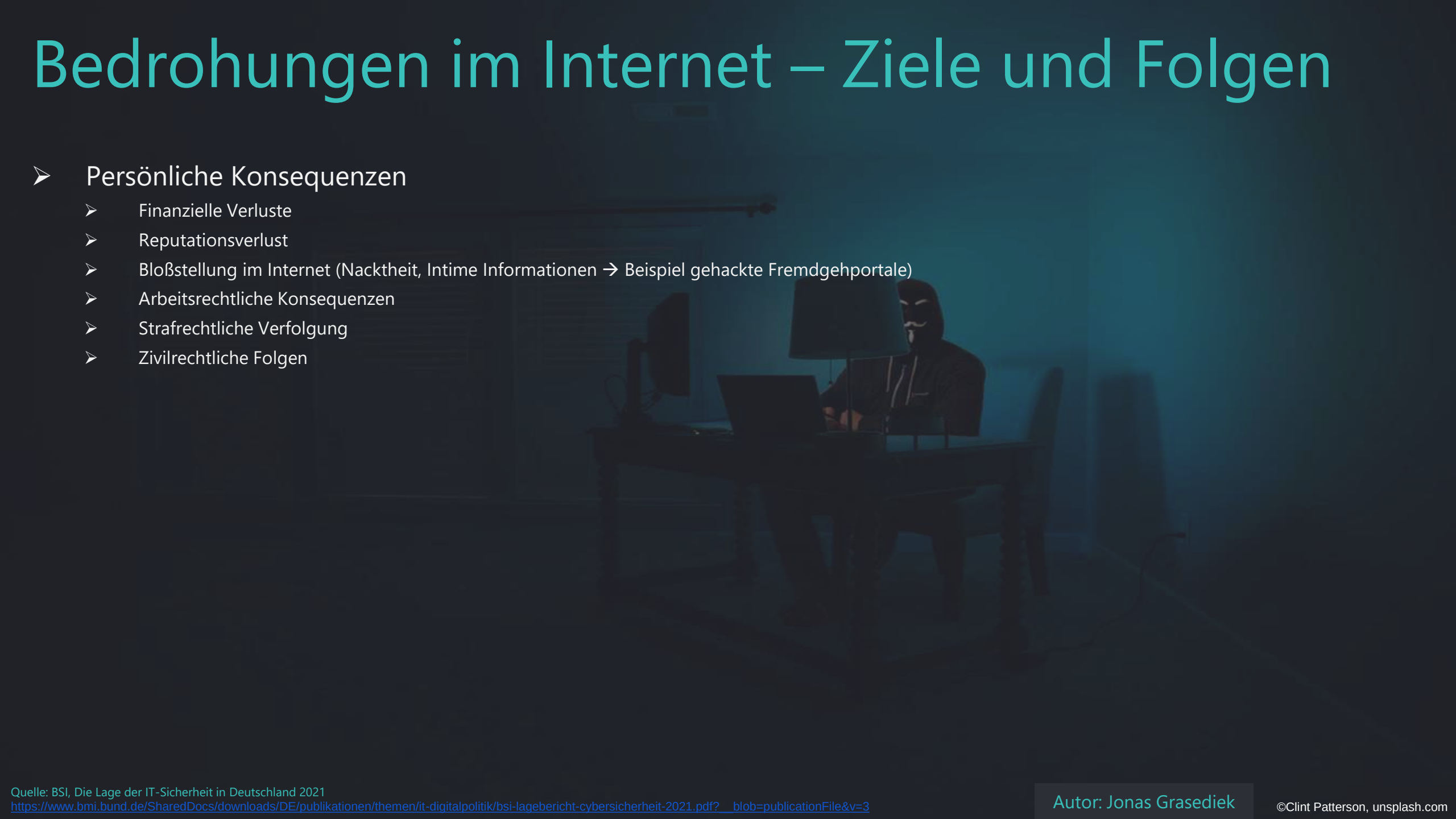


Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2021
https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3

Autor: Jonas Grasediek

# Bedrohungen im Internet – Ziele und Folgen

- Persönliche Konsequenzen
  - Finanzielle Verluste
  - Reputationsverlust
  - Bloßstellung im Internet (Nacktheit, Intime Informationen → Beispiel gehackte Fremdgehportale)
  - Arbeitsrechtliche Konsequenzen
  - Strafrechtliche Verfolgung
  - Zivilrechtliche Folgen



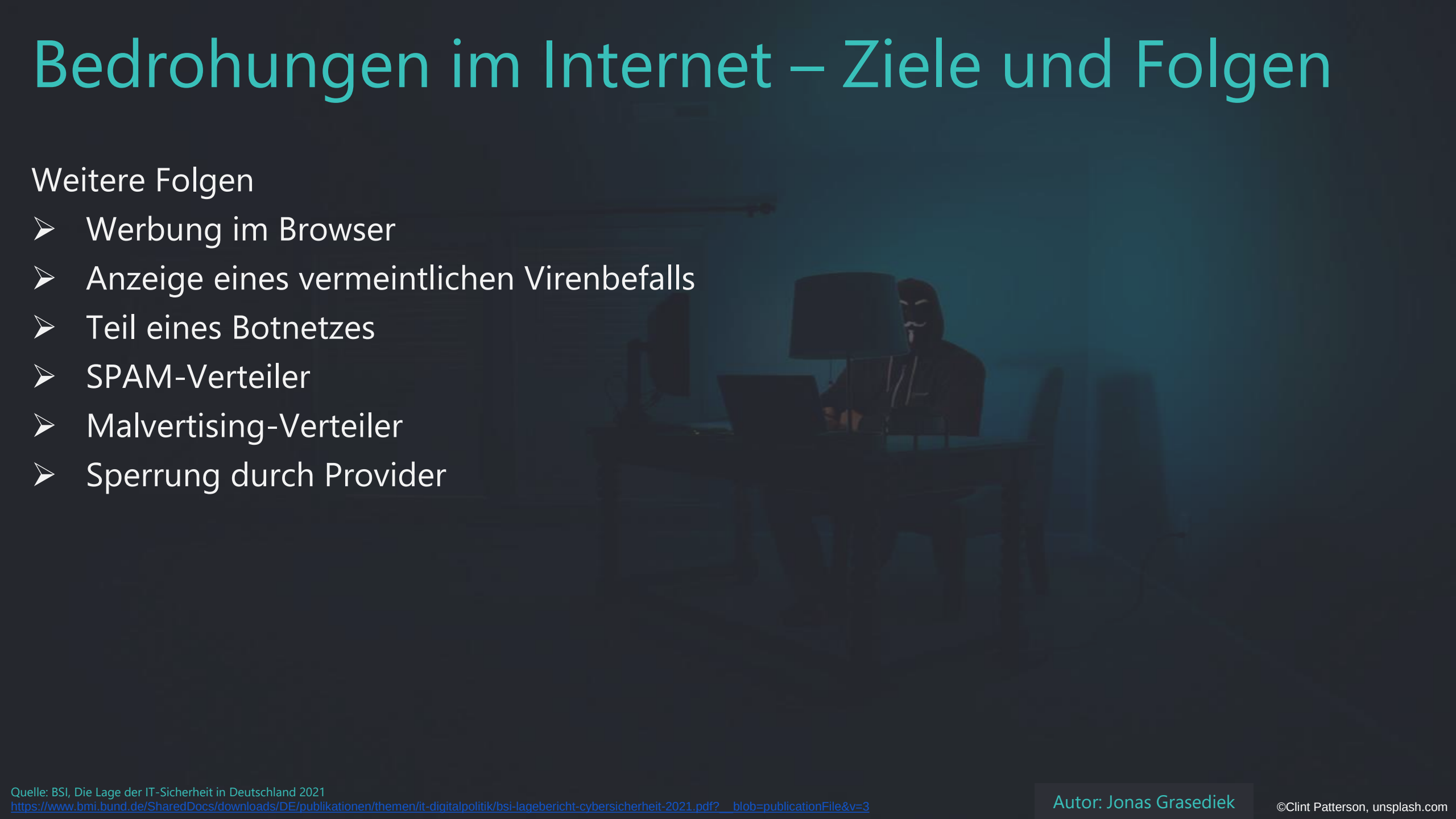
Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2021
https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3

Autor: Jonas Grasediek

# Bedrohungen im Internet – Ziele und Folgen

Weitere Folgen

- Werbung im Browser
- Anzeige eines vermeintlichen Virenbefalls
- Teil eines Botnetzes
- SPAM-Verteiler
- Malvertising-Verteiler
- Sperrung durch Provider

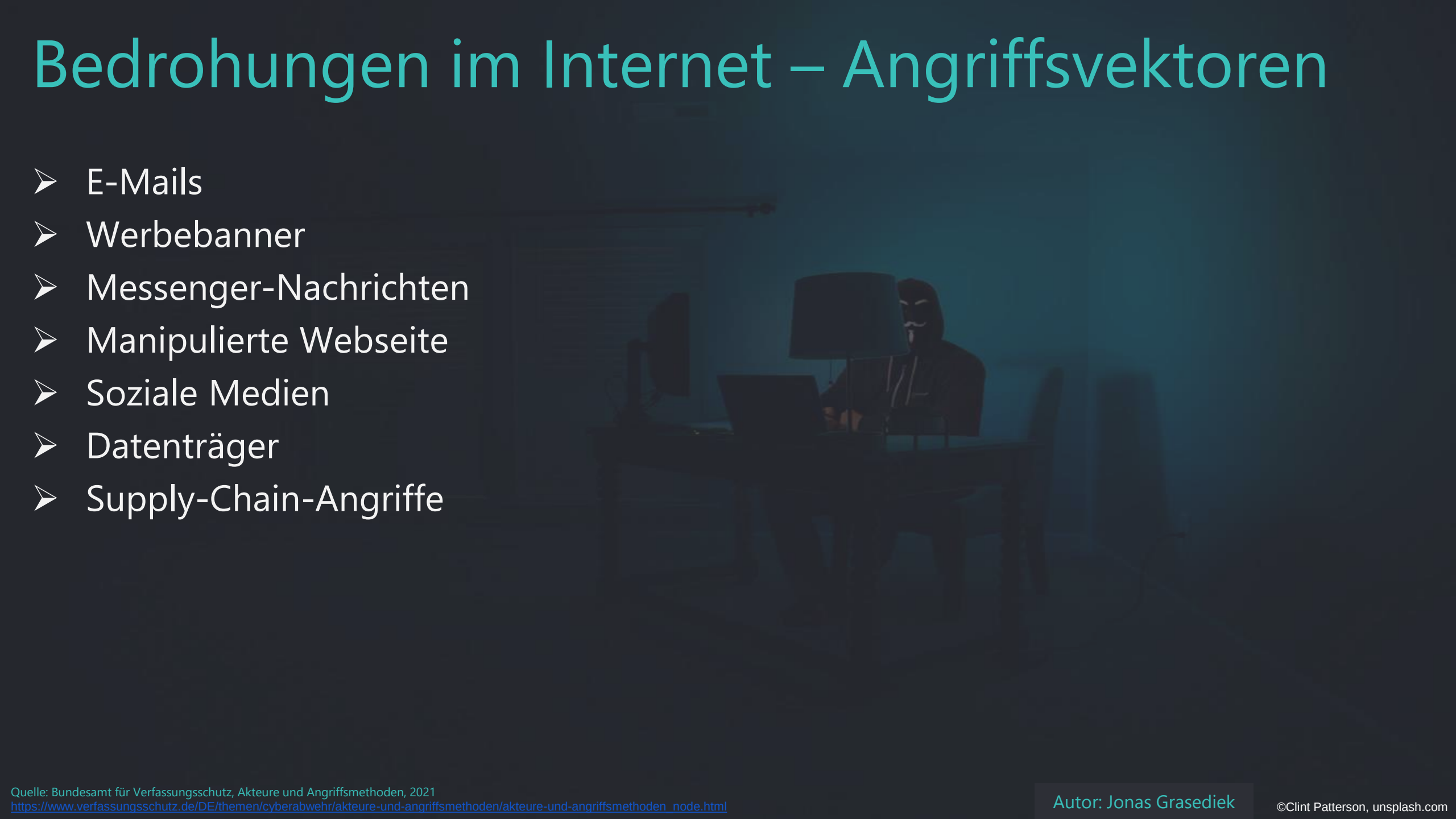


Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2021
https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3

Autor: Jonas Grasediek

# Bedrohungen im Internet – Angriffsvektoren

- E-Mails
- Werbebanner
- Messenger-Nachrichten
- Manipulierte Webseite
- Soziale Medien
- Datenträger
- Supply-Chain-Angriffe



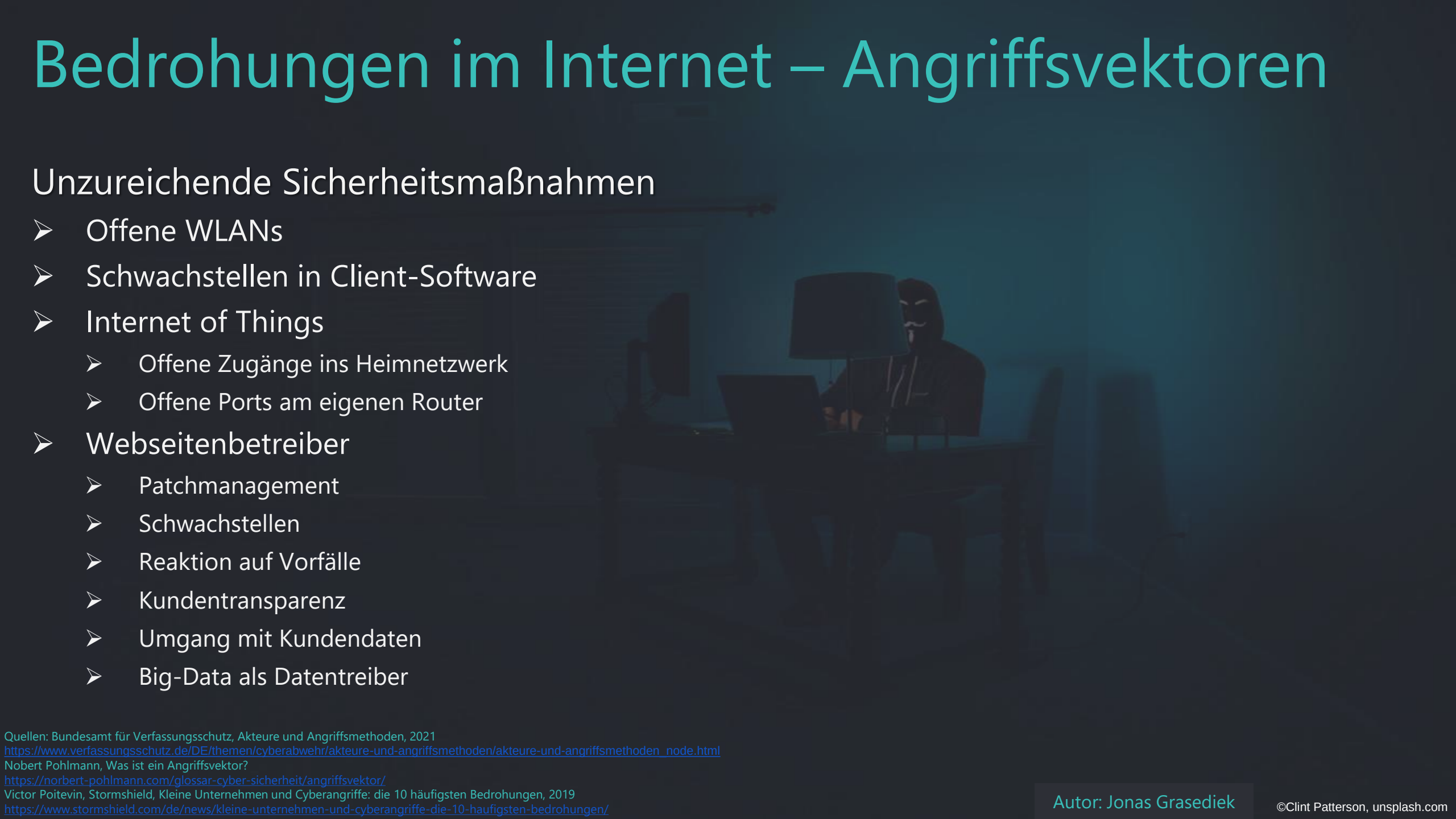
Quelle: Bundesamt für Verfassungsschutz, Akteure und Angriffsmethoden, 2021
https://www.verfassungsschutz.de/DE/themen/cyberabwehr/akteure-und-angriffsmethoden/akteure-und-angriffsmethoden_node.html

Autor: Jonas Grasediek

# Bedrohungen im Internet – Angriffsvektoren

## Unzureichende Sicherheitsmaßnahmen

- Offene WLANs
- Schwachstellen in Client-Software
- Internet of Things
  - Offene Zugänge ins Heimnetzwerk
  - Offene Ports am eigenen Router
- Webseitenbetreiber
  - Patchmanagement
  - Schwachstellen
  - Reaktion auf Vorfälle
  - Kundentransparenz
  - Umgang mit Kundendaten
  - Big-Data als Datentreiber



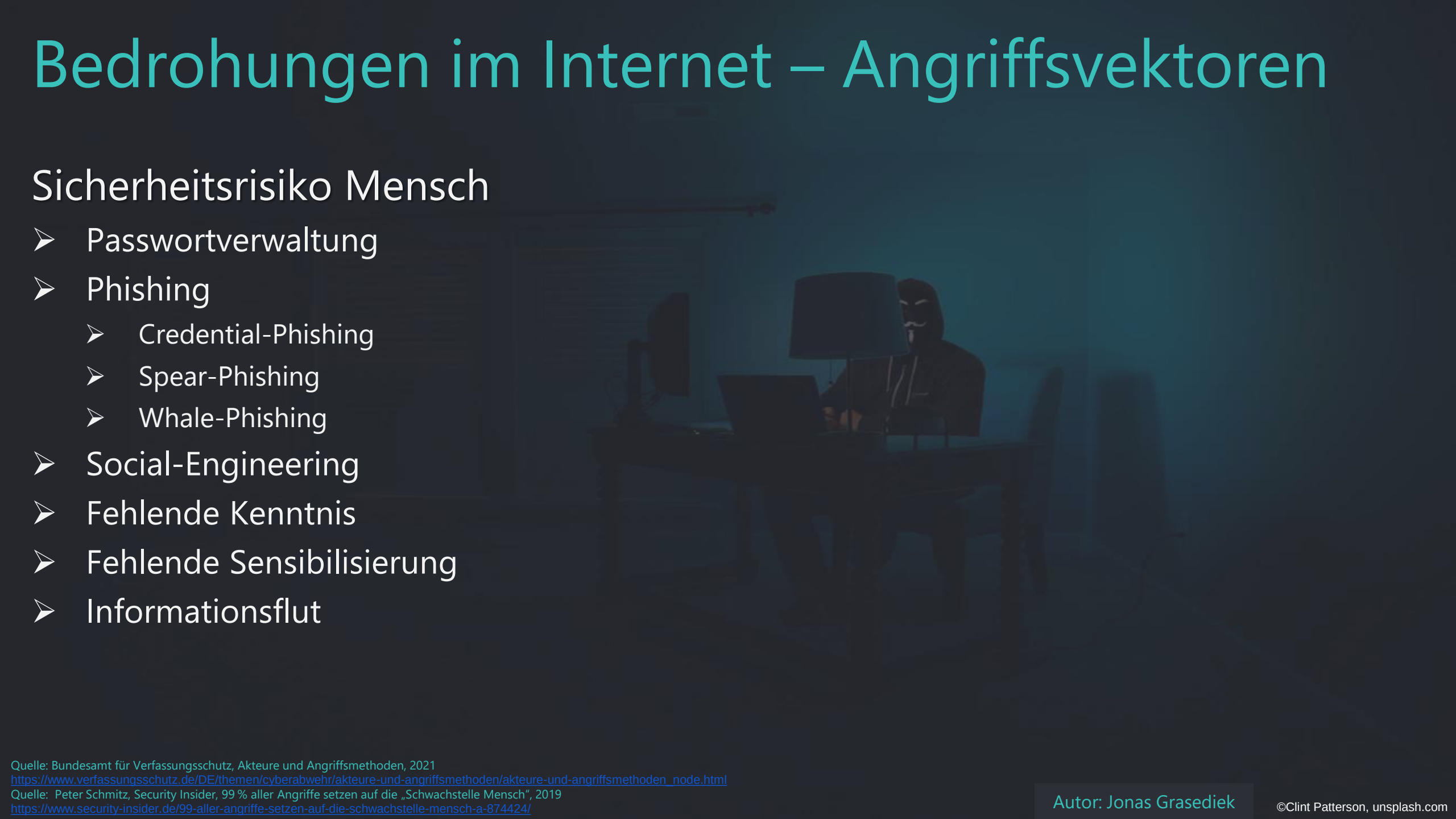
Quellen: Bundesamt für Verfassungsschutz, Akteure und Angriffsmethoden, 2021
https://www.verfassungsschutz.de/DE/themen/cyberabwehr/akteure-und-angriffsmethoden/akteure-und-angriffsmethoden_node.html
Nobert Pohlmann, Was ist ein Angriffsvektor?
https://norbert-pohlmann.com/glossar-cyber-sicherheit/angriffsvektor/
Victor Poitevin, Stormshield, Kleine Unternehmen und Cyberangriffe: die 10 häufigsten Bedrohungen, 2019
https://www.stormshield.com/de/news/kleine-unternehmen-und-cyberangriffe-die-10-haufigsten-bedrohungen/

Autor: Jonas Grasediek

# Bedrohungen im Internet – Angriffsvektoren

## Sicherheitsrisiko Mensch

- Passwortverwaltung
- Phishing
  - Credential-Phishing
  - Spear-Phishing
  - Whale-Phishing
- Social-Engineering
- Fehlende Kenntnis
- Fehlende Sensibilisierung
- Informationsflut



Quelle: Bundesamt für Verfassungsschutz, Akteure und Angriffsmethoden, 2021
https://www.verfassungsschutz.de/DE/themen/cyberabwehr/akteure-und-angriffsmethoden/akteure-und-angriffsmethoden_node.html
Quelle: Peter Schmitz, Security Insider, 99 % aller Angriffe setzen auf die „Schwachstelle Mensch“, 2019
https://www.security-insider.de/99-aller-angriffe-setzen-auf-die-schwachstelle-mensch-a-874424/

Autor: Jonas Grasediek

# Sichere Online-Kommunikation

# Browser – Technische Grundlagen

## Webseitenverschlüsselung

- https://...
- Verschlüsselte Kommunikation zwischen Browser und Webseite
- SSL/TLS-Protokoll
- Zertifikatsbasiert

## Zertifikate

- Öffentlicher + privater Schlüssel
- Prüfung auf gültiges Zertifikat beim Aufruf einer Webseite
- Warnung bei ungültigem Zertifikat
- Öffentlich prüfbare Zertifikatskette
- Aufruf von Webseiten ohne Verschlüsselung nicht mehr unterstützt

Quelle: BSI, SSL/TLS-Protokoll sicher einsetzen
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/Verschluesselung-und-Zertifikate/verschluesselung-und-zertifikate_node.html

Autor: Jonas Grasediek

# Browser – Technische Grundlagen

## Aktive Inhalte

- Programme auf Webseiten, u. a. zuständig für Menüs und eingebettete Inhalte
- Werden auf dem Rechner des Anwenders ausgeführt
- Oftmals ohne Wissen des Anwenders geladen und ausgeführt
- Für den Anwender nicht erkennbar was gefährlich
- Java, JavaScript, ActiveX, Flash, Silverlight, etc.

## Cookies

- Speichert Informationen über den Besuch einer Webseite auf dem Rechner
- Online-Formulare müssen nicht erneut eingegeben werden
- Warenkorb bleibt ohne Anmeldung erhalten
- Keine direkte Gefährdung, da keine ausführbaren Inhalte
- Session Cookies → werden beim Schließen des Browsers gelöscht
- Dauerhafte Cookies → werden über lange Zeiträume gespeichert

Autor: Jonas Grasediek

Quelle: BSI, Der Browser – Gefahren und Risiken
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/Gefahren-und-Risiken/gefahren-und-risiken_node.html

# Wie erkenne ich „unsichere“ Webseiten?

- Auf https achten
- Zertifikat prüfen
- Link zu einer URL prüfen (Mouse-Drag-Over)
- Auf ausführbare Inhalte achten, ggf. Warnmeldung vom Browser
  - Testseite → https://www.whatismybrowser.com/detect/is-javascript-enabled

- Tools zur Prüfung der Webseitensicherheit verwenden
  - Google Transparenzbericht, Virustotal, Hybrid-Analysis
  - Technischere Analysen mit ANY RUN

- Kein blindes Vertrauen in “Vertrauensplaketten”

- Weitere Anzeichen für eine unsichere Webseite
  - Sofortige Redirects
  - Browser-Warnungen

Autor: Jonas Grasediek

# Wie kann ich mich schützen?

- Aktive Inhalte blockieren
  - **Chrome:** Einstellungen > Erweitert > Sicherheit und Datenschutz
  - **Edge:** Einstellungen > Erweiterte Einstellungen
  - **Firefox:** Extras > Einstellungen > Datenschutz & Sicherheit
  - **Safari:** Einstellungen > Datenschutz
- Mehrere Browser → BSI Browser-Abgleichstabelle zum Mindeststandard des BSI für sichere Web
- Antivirenprogramm
- Regelmäßige Updates
- Browser-Erweiterungen
  - Facebook Container, Adblocker, PrivacyBadger
  - Firefox Monitor
- Browsereinstellungen testen
  - PANOPTICLICK 3.0 → https://panopticlick.eff.org/

Quelle: BSI, Das Internet sicher nutzen – 10 Tipps zur sicheren Nutzung des Internets
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Brosch_A6_Surfen_aber_sicher.pdf?__blob=publicationFile&v=3

Autor: Jonas Grasediek

# Wie kann ich mich schützen?

- Alle nicht benötigten Cookies ablehnen
- Anonymes / privates Browsen
- VPN-Dienste
- Offline Passwortsafe verwenden, z. B. KeePass
- 2-Faktor-Authentifizierung / FIDO2 einsetzen
- Sandbox / Virtuelle Maschinen
- Grundsätzliches Misstrauen
- Informieren

Quelle: BSI, Das Internet sicher nutzen – 10 Tipps zur sicheren Nutzung des Internets
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Brosch_A6_Surfen_aber_sicher.pdf?__blob=publicationFile&v=3

Autor: Jonas Grasediek

# Wie kann ich mich schützen?

## Datensicherung?

Autor: Jonas Grasediek

# E-Mails

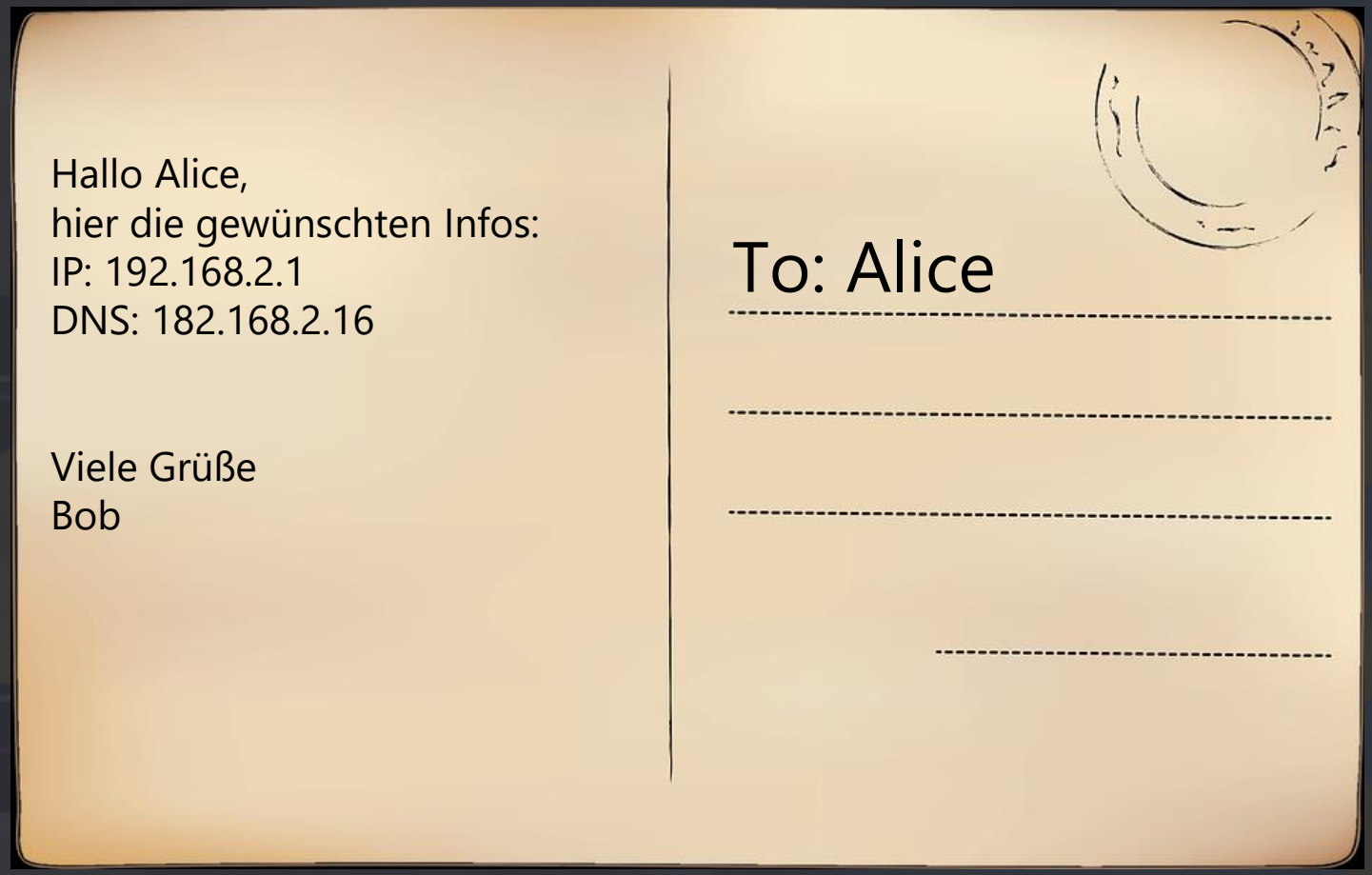
# E-Mails


**E-Mails sind nicht als Brief zu verstehen …**

Autor: Jonas Grasediek

# E-Mails

**... sondern als Postkarte, da sie grundsätzlich für jeden einsehbar sind.**

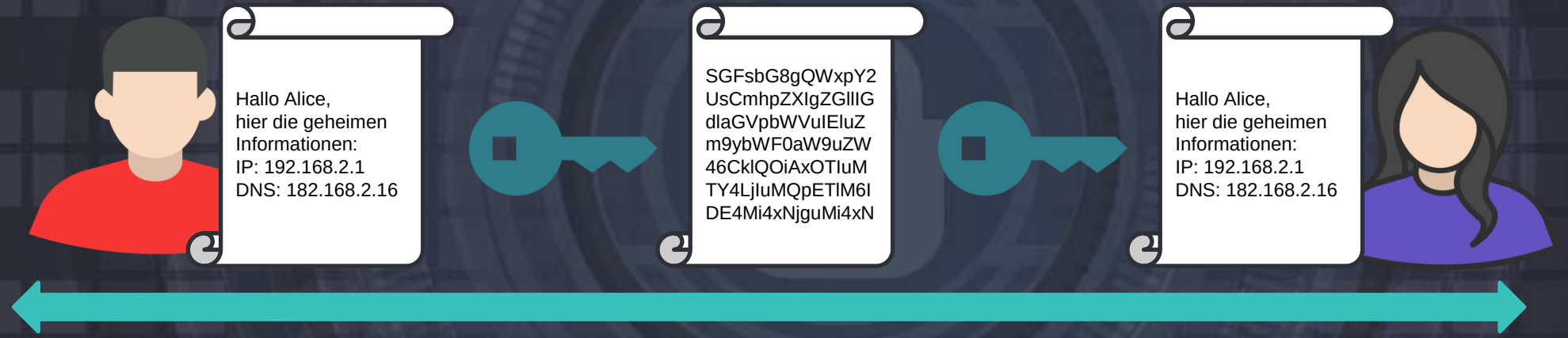



**Der Transportweg zum E-Mail-Provider wird zwar verschlüsselt, nicht aber der Inhalt der eigentlichen E-Mail!**

Autor: Jonas Grasediek

# Grundlagen der Verschlüsselung

## Symmetrische Verschlüsselung

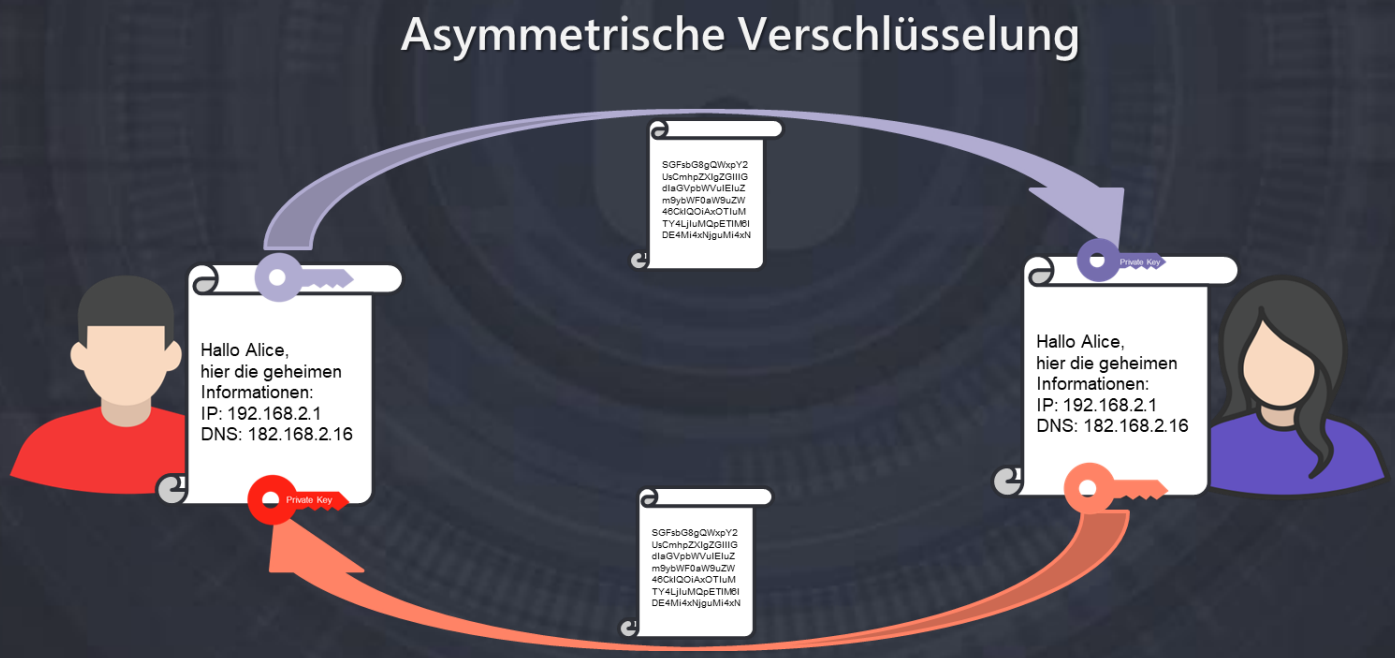



Quelle: BSI für Bürger, Symmetrische Verschlüsselung
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesseltkommunizieren/Grundlagenwissen/SymmetrischeVerschluesselung/symmetrische_verschluesselung_node.html

Autor: Jonas Grasediek

# Grundlagen der Verschlüsselung

**Verschlüsseln** immer mit dem **Public Key** des Empfängers
**Entschlüsseln** immer mit dem **Private Key** des Empfängers



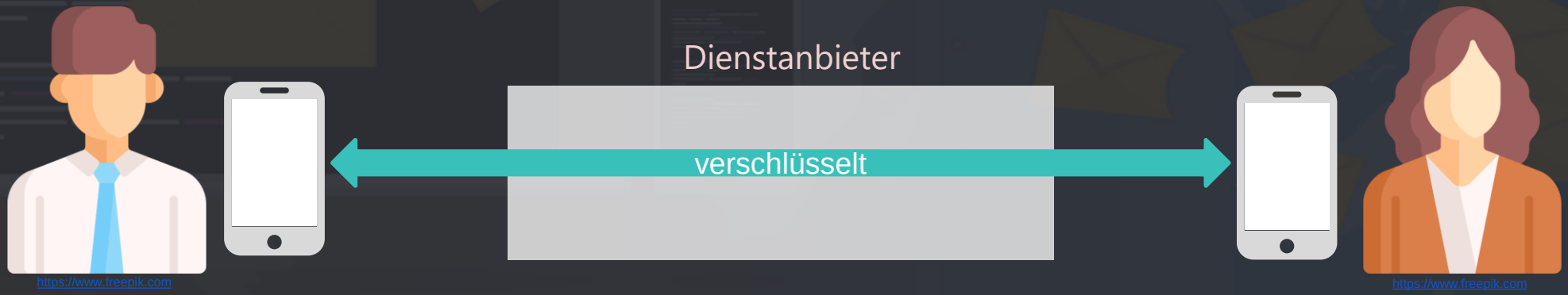

Autor: Jonas Grasediek

Quelle: BSI für Bürger, Asymmetrische Verschlüsselung
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesseltkommunizieren/Grundlagenwissen/AsymmetrischeVerschluesselung/asymmetrische_verschluesselung_node.html

# Grundlagen der Verschlüsselung

## Transportverschlüsselung


## Ende-zu-Ende-Verschlüsselung




Quelle: Dr. Datenschutz, OpenPGP & S/MIME – Begriffe der E-Mail-Verschlüsselung, 2016
https://www.dr-datenschutz.de/openpgp-smime-begriffe-der-e-mail-verschluesselung/

Autor: Jonas Grasediek

# E-Mails - Grundlagen

- Vertraulichkeit
  - Schutz vor unbefugter Preisgabe von Informationen
  - Daten sind ausschließlich berechtigten Personen zugänglich
  - **Verschlüsselung**

- Integrität (inkl. Authentizität)
  - Sicherstellung der Korrektheit (Unversehrtheit) von Daten
  - Schutz vor unbefugter Veränderung der Daten
  - Änderungen an Daten, Angaben zum Autor oder Zeitstempel auf dem Transportweg führen zum Verlust der Integrität
  - **Signatur**

Quelle: BSI, Cyber-Glossar, Buchstabe V
https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/Functions/glossar.html?nn=520190&cms_lv2=132818
Quelle: BSI, Cyber-Glossar, Buchstabe I
https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/Functions/glossar.html?nn=520190&cms_lv2=132764

Autor: Jonas Grasediek

# E-Mails – Verschlüsselung / Signatur

- Verschlüsselung
  - Absender
    - Verschlüsselt seine Nachricht mit dem öffentlichen Schlüssel des Empfängers
  - Nachricht an den Empfänger versendet
  - Empfänger
    - Entschlüsselt die Nachricht mit eigenem privaten Schlüssel

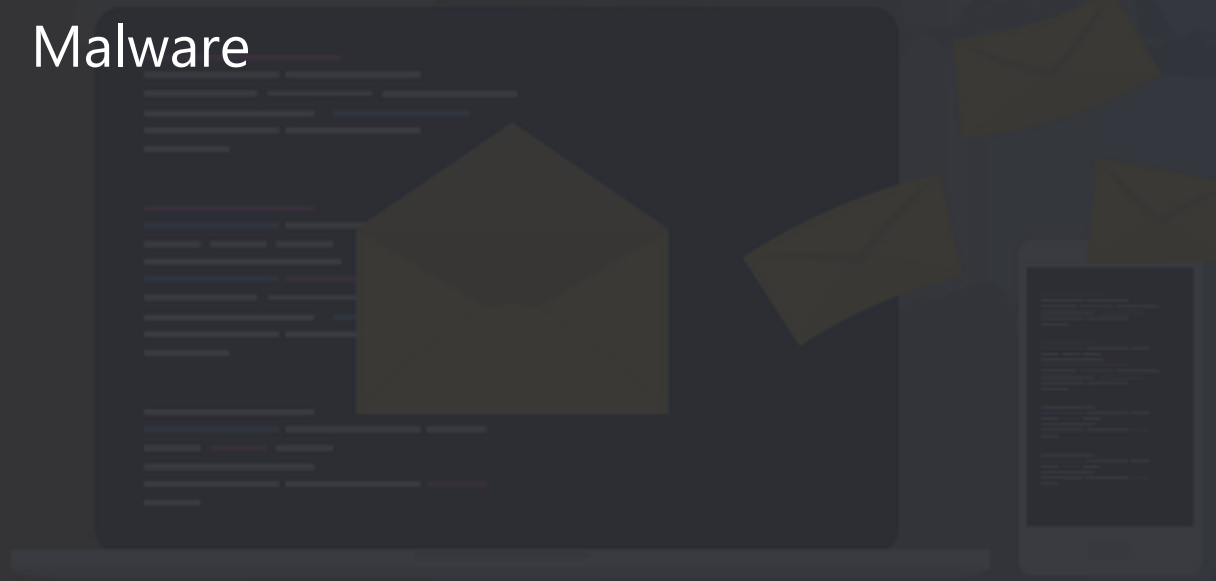
- Signatur
  - Absender
    - berechnet Hashwert aus seiner Nachricht
    - Verschlüsselt den Hashwert mit seinem privaten Schlüssel (=digitale Signatur)
  - Nachricht wird zusammen mit dem verschlüsselten Hashwert an den Empfänger versendet
  - Empfänger
    - erstellt ebenfalls einen Hashwert der erhaltenen Nachricht (selbe Hashfunktion)
    - entschlüsselt den erhaltenen Hashwert mit dem öffentlichen Schlüssel (des Absenders) und vergleicht beide Werte miteinander.

Quelle: Dr. Datenschutz, Hashwerte und Hashfunktionen einfach erklärt, 2016
https://www.dr-datenschutz.de/hashwerte-und-hashfunktionen-einfach-erklaert/

Autor: Jonas Grasediek

# E-Mails – typische Gefahren

- SPAM
- Phishing
- Malware



Autor: Jonas Grasediek

# Wie erkenne ich unsichere Mails?

- Eingang einer Mail von Unbekannten
- Unerwartete Mails
- Mails mit Aufforderung einen bestimmten Link anzuklicken
- Mails mit unerwarteten Anhängen
- Mails mit Aufforderung einen bestimmten Anhang zu öffnen
- Sehr schlechte Rechtschreibung / Grammatik
  Hinweis auf maschinelle Übersetzung?
- Rechnung zu Dingen die nicht bestellt wurden
- Vermeintliche Benachrichtigungen über
  - Single-Damen aus dem Ausland
  - Überraschendes Erbe, Vermögensverwaltung im Ausland
  - Gewinnspiele / Preisausschreiben
  - Ausschüttung von Geldern, Aktien, etc.
  - Angelblich lange vermisste Freunde, Verwandte, etc.

Quelle: keepnetlab, 10 Email Security Risks in 2020
https://www.keepnetlabs.com/anti-phishing-solution-threat-simulation-2/

Autor: Jonas Grasediek

# E-Mail-Sicherheits-Irrtümer

- Wenn ich eine E-Mail nur anschaue aber keinen Anhang öffne, kann nix passieren
  - Bei E-Mails im HTML-Format kann Schadcode im zugrundeliegenden Code versteckt sein

- Man kann in Spam-Mails den Link zum Löschen aus dem Verteiler anklicken
  - SPAM-Mails werden häufig dazu verwendet festzustellen, ob die Adresse gültig ist und ob jemand aktiv damit arbeitet
  - Ein Klick auf den Link bestätigt dem potentiellen Angreifer, dass die Adresse funktioniert
  - Folge: noch mehr SPAM und ggf. Schadcode-Mails → Vorbereitung weiterer Angriffe

- Eine E-Mail kommt immer von der Adresse, die im Absender-Feld steht
  - Das ist **FALSCH**
  - Mit der Maus über den Absender fahren gibt einen ersten Hinweis auf die wahre Identität
  - Die Echtheit des Absenders lässt sich nur durch eine Prüfung des Mailheaders feststellen

- Phishing-Mails sind leicht zu erkennen
  - Das ist **FALSCH**
  - Phishing-Mails werden zunehmend besser bzw. professioneller
  - Die Echtheit einer solchen Mail lässt sich im Zweifel auch durch eine Prüfung des Mailheaders feststellen

Autor: Jonas Grasediek

Quelle: BSI, Sicherheits-Irrtümer: E-Mail-Sicherheit, 2021
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Sicherheitsirrtuemer/irrtuemer-e-mail-sicherheit.html

# Wie kann ich mich schützen?

- Mehrere E-Mail-Adressen verwenden (Beispiel)
  - GMX für Online-Shopping
  - GMAIL für Soziale Netzwerke
  - LIVE / Onedrive für Dateiaustausch
  - Weitere Anbieter für SPAM-Adressen
  - **Für einmalige Dinge Wegwerfadressen benutzen**
- Verschlüsseln und Signieren
  - Gut: E-Mails signieren
  - Besser: E-Mails verschlüsseln
  - Noch Besser: E-Mails verschlüsseln und signieren
- Sandbox / Virtuelle Maschinen benutzen
  - VirtualBox, Hyper-V, Vmware Player
  - Quemu, Parallels
- Links / Anhänge bei Dienstleistern zur Prüfung hochladen
- Dateierweiterungen in Windows anzeigen
- Virenscanner installieren
- Regelmäßige Updates

Quellen: NOMORERANSOM.ORG, Tipps zur Vorbeugung
https://www.nomoreransom.org/de/prevention-advice.html
BSI, Nutzen Sie die E-Mail wirklich sicher?, 2021
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/E-Mail-Sicherheit/e-mail-sicherheit_node.html;jsessionid=788A97CF60DABF78441602712521FBD5.internet471

Autor: Jonas Grasediek

# Wie kann ich mich schützen?

Misstrauisch sein

Datensicherung?

Autor: Jonas Grasediek

# Smartphones

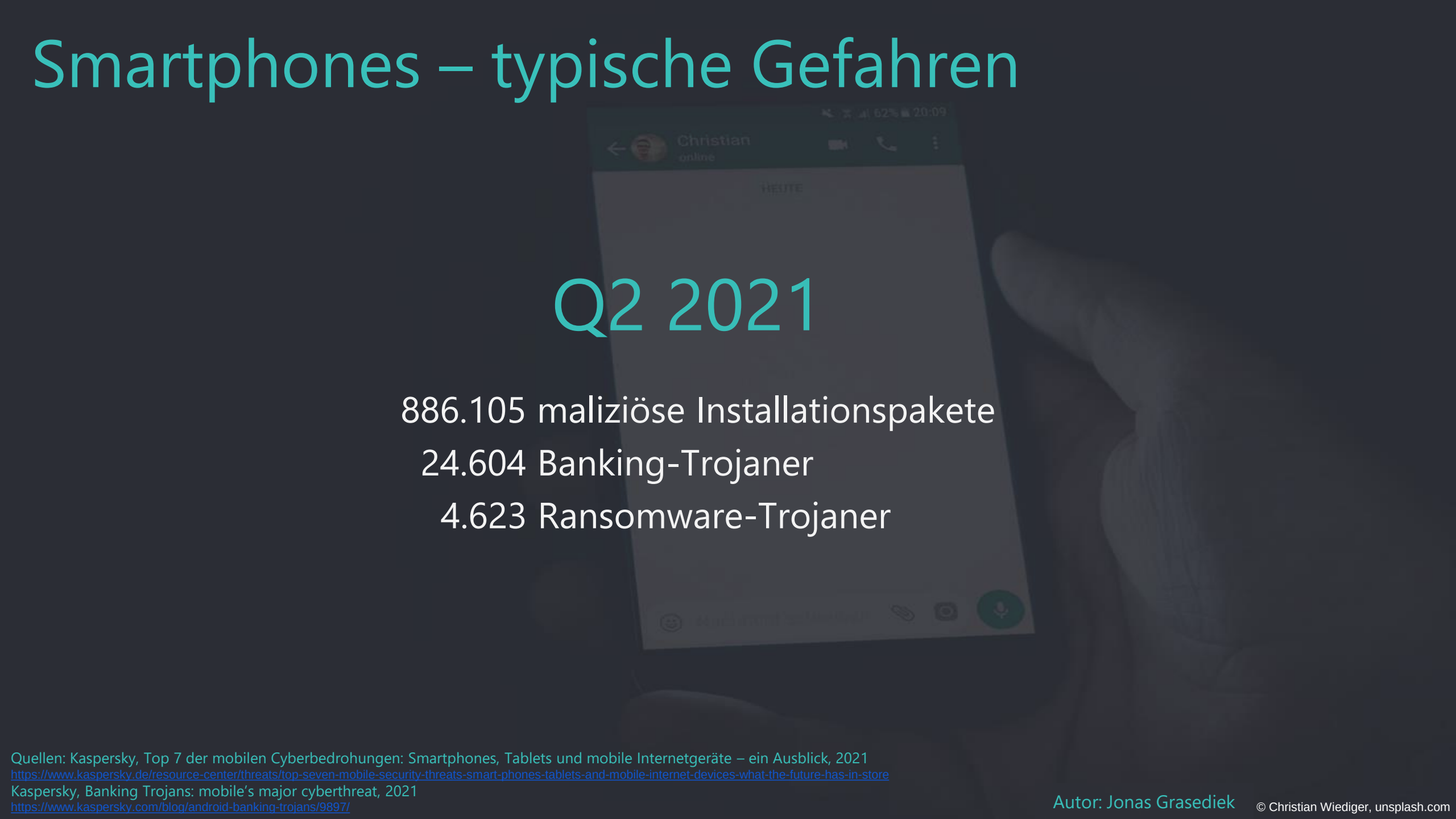
# Smartphones – typische Gefahren

- „Riskware“
- Unsichere WLANs
- Banking-Trojaner
- Ransomware
- Trojaner-SMS
- Backdoor
- Netzwerk-Spoofing
- Cybersquatting
- Phishing-Angriffe
- Spyware
- Entschlüsselte Kryptografie
- AdWare
- Fehlerhaftes Session-Handling


Quellen:
Kaspersky, Top 7 der mobilen Cyberbedrohungen: Smartphones, Tablets und mobile Internetgeräte – ein Ausblick, 2021
https://www.kaspersky.de/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store
Kaspersky, Banking Trojans: mobile’s major cyberthreat, 2021
https://www.kaspersky.com/blog/android-banking-trojans/9897/
Securelist, IT threat evolution in Q2 2021. Mobile statistics, 2021
https://securelist.com/it-threat-evolution-q2-2021-mobile-statistics/103636/

Autor: Jonas Grasediek

# Smartphones – typische Gefahren



## Q2 2021

886.105 maliziöse Installationspakete

24.604 Banking-Trojaner

4.623 Ransomware-Trojaner

Quellen: Kaspersky, Top 7 der mobilen Cyberbedrohungen: Smartphones, Tablets und mobile Internetgeräte – ein Ausblick, 2021
https://www.kaspersky.de/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store
Kaspersky, Banking Trojans: mobile's major cyberthreat, 2021
https://www.kaspersky.com/blog/android-banking-trojans/9897/

Autor: Jonas Grasediek

# Smartphones – Wie kann ich mich schützen?

- Basisschutz sicherstellen
  - Einschalten der vorhandenen Sicherheitsfunktionen
  - PIN nach Bildschirmsperre
  - PIN nach Gerätestart
  - Automatische Updates aktivieren (z.B. im WLAN)
  - Gerät nicht aus den Augen lassen und keinem Fremden geben

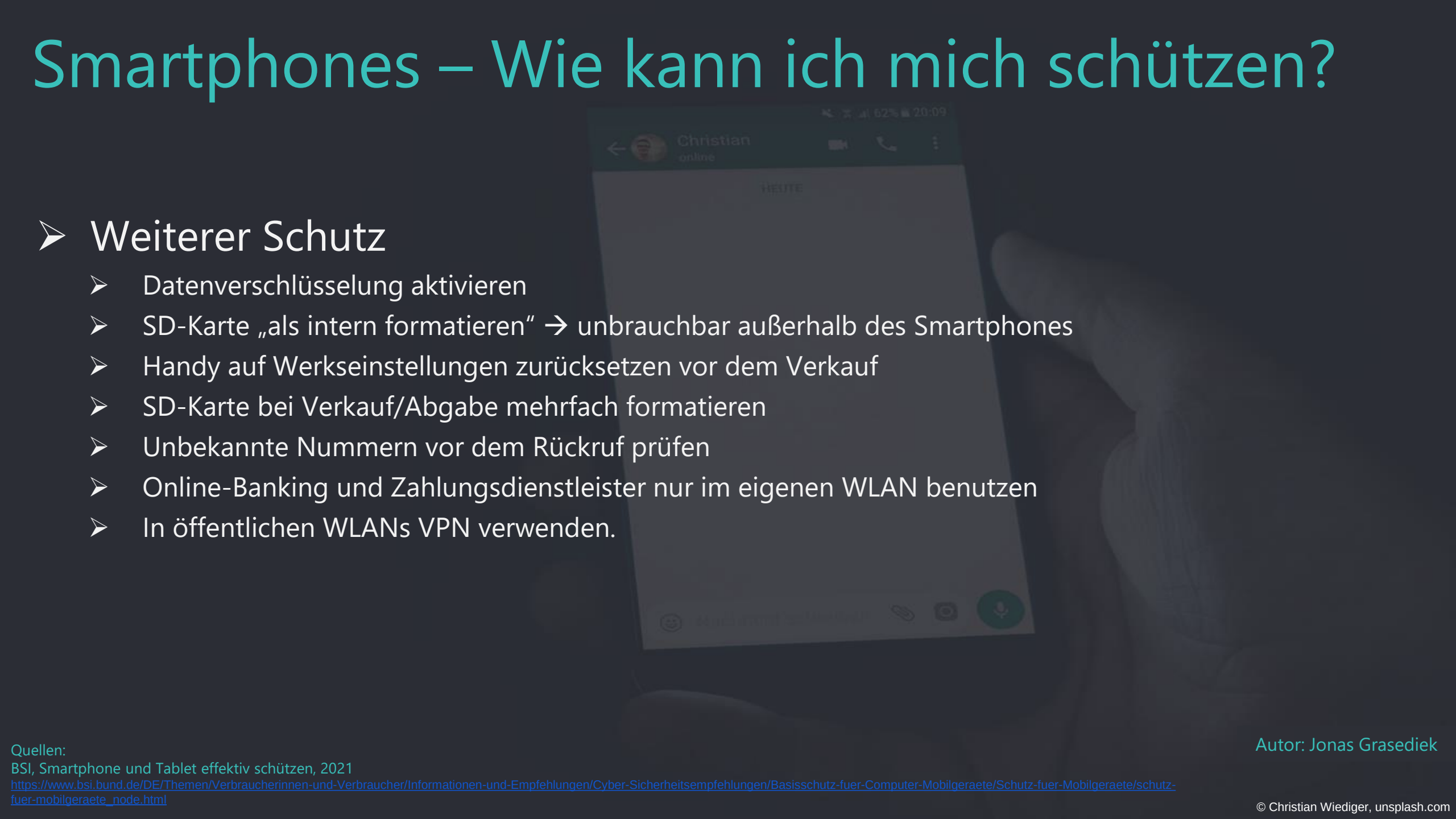
- App-Sicherheit
  - Installation nur aus vertrauenswürdigen Quellen
  - Nur Apps installieren, die benötigt werden
  - Verifikation der Echtheit durch kurze Internetrecherche möglich
  - Deinstallation von Apps die nicht verwendet werden
  - Prüfen und Einschränken von Zugriffsrechten

- Schnittstellen-Sicherheit
  - Aktivierung nur im Bedarfsfall
  - Prüfen ob Schnittstelle immer aktiviert sein muss
  - Keine öffentlichen / fremden USB-Schnittstellen zum Laden verwenden

Quellen:
BSI, Smartphone und Tablet effektiv schützen, 2021
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Basisschutz-fuer-Computer-Mobilgeraete/Schutz-fuer-Mobilgeraete/schutz-fuer-mobilgeraete_node.html

Autor: Jonas Grasediek

# Smartphones – Wie kann ich mich schützen?

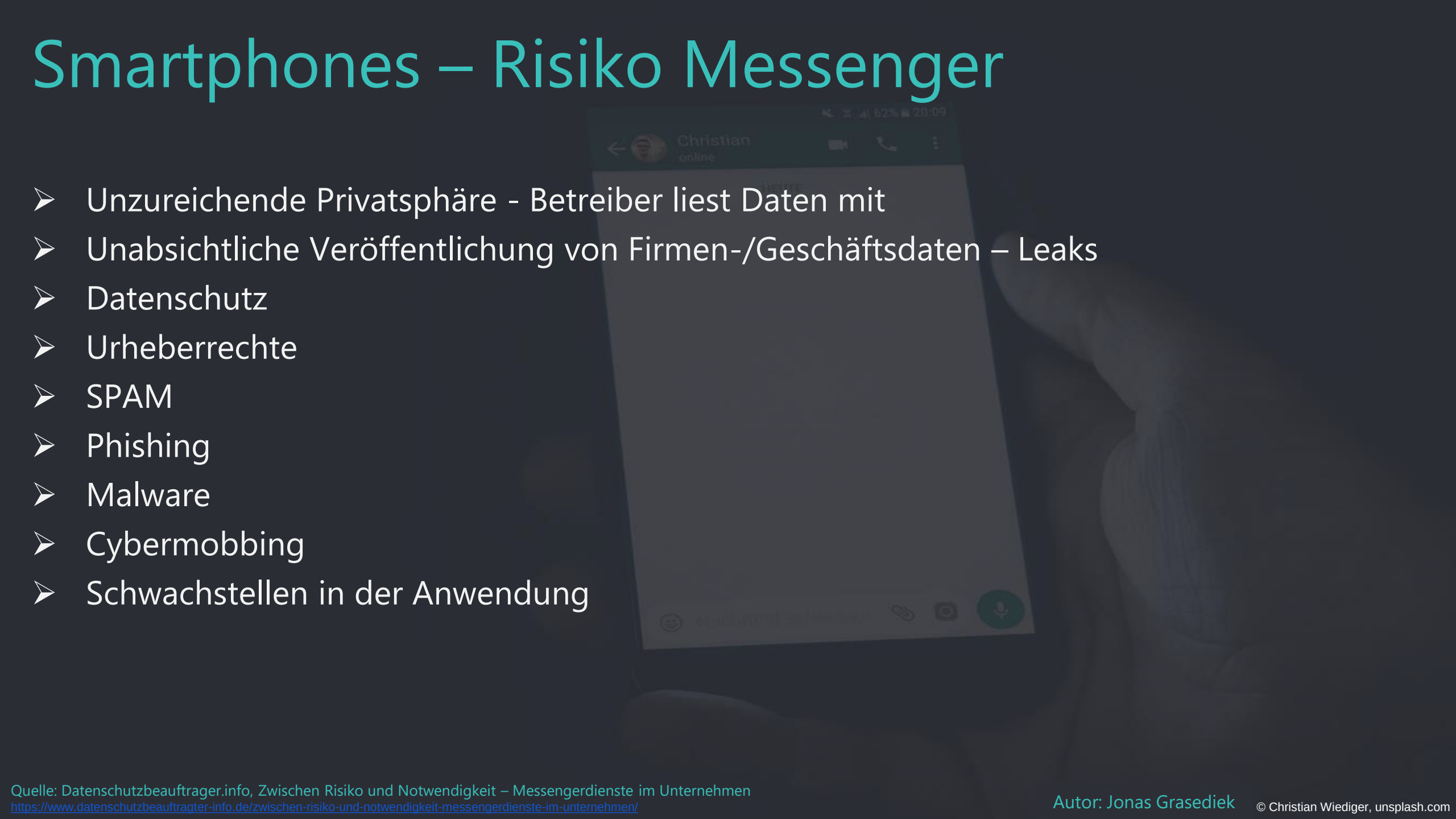


- Weiterer Schutz
  - Datenverschlüsselung aktivieren
  - SD-Karte „als intern formatieren“ → unbrauchbar außerhalb des Smartphones
  - Handy auf Werkseinstellungen zurücksetzen vor dem Verkauf
  - SD-Karte bei Verkauf/Abgabe mehrfach formatieren
  - Unbekannte Nummern vor dem Rückruf prüfen
  - Online-Banking und Zahlungsdienstleister nur im eigenen WLAN benutzen
  - In öffentlichen WLANs VPN verwenden.

Quellen:
BSI, Smartphone und Tablet effektiv schützen, 2021
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Basisschutz-fuer-Computer-Mobilgeraete/Schutz-fuer-Mobilgeraete/schutz-fuer-mobilgeraete_node.html

Autor: Jonas Grasediek

# Smartphones – Risiko Messenger



- Unzureichende Privatsphäre - Betreiber liest Daten mit
- Unabsichtliche Veröffentlichung von Firmen-/Geschäftsdaten – Leaks
- Datenschutz
- Urheberrechte
- SPAM
- Phishing
- Malware
- Cybermobbing
- Schwachstellen in der Anwendung

Quelle: Datenschutzbeauftrager.info, Zwischen Risiko und Notwendigkeit – Messengerdienste im Unternehmen
https://www.datenschutzbeauftragter-info.de/zwischen-risiko-und-notwendigkeit-messengerdienste-im-unternehmen/

Autor: Jonas Grasediek

# Messenger – WhatsApp-Problematik

- Nutzerunfreundliche Geschäftspolitik
  - Firmensitz für EU in Irland → Datenschutz, Steuern …
  - Facebook musste gerichtlich dazu gezwungen werden, die AGBs für WhatsApp auf Deutsch zu veröffentlichen (Aktenzeichen: 5 U 156/14)
  - Facebook kann sich nicht darauf berufen, Gerichtsbeschlüsse in deutscher Sprache nicht zu verstehen (Aktenzeichen: I-7 W 66/19)
- Zugriff
  - Fotos, Adressbuch
  - Kamera, Mikrofon
  - Standort
  - **Laufende Apps**
- Bezahlung mit den eigenen Daten
- Daten liegen auf den Servern eines amerikanischen Unternehmens → CLOUD / Freedom Act
- Ende-zu-Ende Verschlüsselung?
- Telegram → Russland erzwingt die Herausgabe der Keys aller Nutzer (2018)

Datenschutz.org, WhatsApp-Datenschutz: Was User wissen sollten
https://www.datenschutz.org/whatsapp-datenschutz/
Quelle: Datenschutz.org, Russia orders Telegram to hand over users' encryption keys, 2018
https://www.theverge.com/2018/3/20/17142482/russia-orders-telegram-hand-over-user-encryption-keys

Autor: Jonas Grasediek

# Messenger – Tipps für mehr Sicherheit

- Lesen sie die AGB und die Datenschutzbestimmungen → Was geschieht mir Ihren Daten?
- Messenger ohne Verknüpfung zu sozialen Medien verwenden
- Datenschutzeinstellungen
  - Zuletzt online
  - Nachricht gelesen – Zeitstempel
  - Weitere Optionen, die etwas über Ihr Verhalten preisgeben
- Tests und Vergleiche heranziehen
  - EFF – Secure Messaging Scorecard https://www.eff.org/de/node/101713/
  - Securemessangingapps.com – SECURE MESSAGING APPS COMPARISON https://www.securemessagingapps.com/
- Rechte des Messengers möglichst begrenzen
- Verschlüsselung an drei Stellen
  - Transportverschlüsselung
  - Ende-zu-Ende-Verschlüsselung
  - Verschlüsselte Speicherung auf dem Endgerät
  - Schlüsselaustausch möglichst persönlich, z. B. via QR-Code
- Trennen Sie geschäftliche von privater Kommunikation
- Blockieren Sie Kontakte über deren Identität Sie sich unsicher sind
- Alle Informationen die Sie versenden, können weitergeleitet werden

Autor: Jonas Grasediek

Quelle: BSI, Messenger & Videotelefonie sicher nutzen, 2021
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Chat-Messenger/Messenger/messenger-sicher-nutzen.html#:~:text=%2Drisiko.net)-,Worauf%20Sie%20bei%20Messengern%20achten%20sollten,der%20Privatsph%C3%A4re%20unterscheiden%20sich%20weltweit.