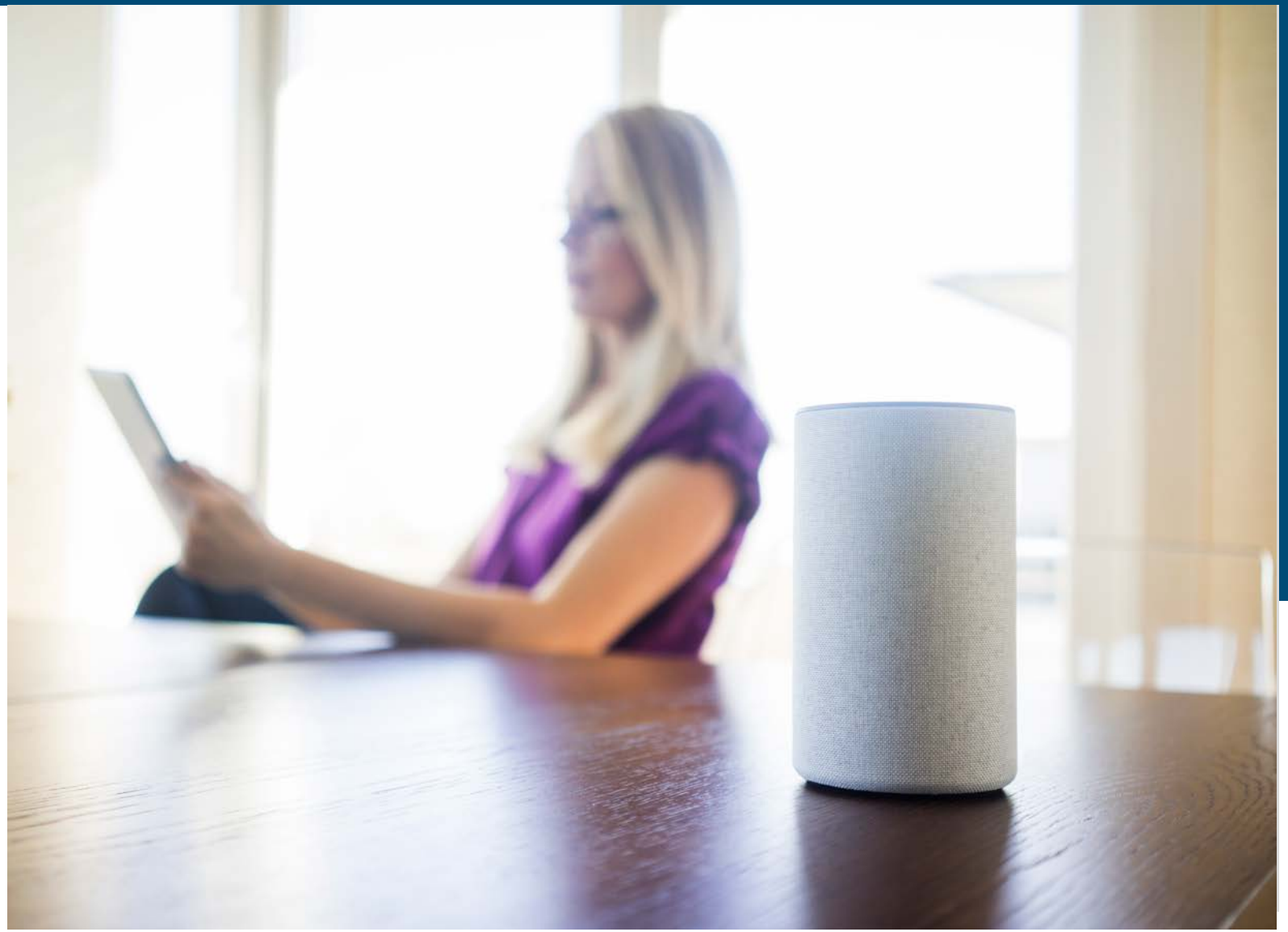
Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mit IT-Sicherheit gegen Digitale Gewalt: Tech Abuse vorbeugen und abwehren

Dr. Katharina Witterhold, Cottbus, 11.06.2024

1. Einleitung
2. Digitale Gewalt und Coercive Control
3. Strategien und Taktiken der Angreifer
4. Maßnahmen und nächste Schritte



© Westend / 61/ Getty Images

Digitale Gewalt – ein weites Feld

© gpointstudio Fotolia

Hate Speech

© highwighstarz Fotolia

Cybermobbing und Cybergrooming

© 1001 color Fotolia

Coercive Control

Digitale Gewalt: Definitorische Lücken

Unter Cyber-Gewalt wird Gewalt verstanden, die sich technischer Hilfsmittel bedient oder die im digitalen Raum stattfindet. Mädchen und Frauen sind besonders stark von Cyber-Gewalt betroffen. Cyber-Gewalt kann von bekannten Tätern und Täterinnen (Partner, Arbeitskollege) und unbekannten Personen im Internet ausgeübt werden. (Bundeskanzleramt Österreich)

Digitale Gewalt geschieht überall dort, wo sich Menschen online treffen, austauschen und vernetzen. Sie reicht von Cybermobbing und Hatespeech über Cyberstalking bis zum Cybergrooming: der Kontaktaufnahme zu Kindern im Internet mit dem Ziel, sie sexuell zu missbrauchen. Oft geschieht digitale Gewalt eng vernetzt mit Angriffen in der physischen Welt. (Bayern-gegen-Gewalt)

Digitale Gewalt ist ein Oberbegriff für Formen von geschlechtsspezifischer Gewalt, die sich technischer Hilfsmittel und digitaler Medien (Handy, Apps, Internetanwendungen, Mails etc.) bedienen und/oder geschlechtsspezifische Gewalt, die im digitalen Raum, z.B. auf Online-Portalen oder sozialen Plattformen stattfindet. Digitale Gewalt funktioniert nicht getrennt von „analoger Gewalt“, sie stellt meist eine Ergänzung oder Verstärkung von Gewaltverhältnissen und -dynamiken dar. (Bundesverband Frauenberatungsstellen)

Damit Bürgerinnen und Bürger die Chancen digitaler Technologien nutzen können, müssen sie sich sicher und selbstbestimmt in einer digitalisierten Umgebung bewegen. Sie müssen neben den Chancen auch die Risiken digitaler Technologien erkennen, bewerten und die Herausforderungen durch eigenes Handeln wirksam bewältigen können.
Cybersicherheitsstrategie für Deutschland (2021)

Hintergrund: Coercive Control und Gewalt

- **Zwanghaftes Kontrollverhalten:** Missbräuchliche Handlungen wie physische Angriffe, Verletzung der IT-Sicherheit, Eindringen in die Privatsphäre etc. um eine Person fügsam zu machen, unterzuordnen und/oder abhängig zu machen. Führt zu limitierter Autonomie bei betroffener Person mit entsprechenden psychischen, physischen, sozialen und finanziellen Folgen.
- **Coercive Control im Kontext digitaler Gewalt**: Angreifer ist meist kein Unbekannter. Fokus besonders auf Partnerschaften, aber auch andere Konstellationen bekannt. Durch Digitalisierung Zunahme von Überwachungs- und Kontrollmöglichkeiten auch im sozialen Nahbereich durch u.a. Tracker, Smarte Türschlösser, smarte Heizungsthermostate, Videosysteme, Router, Smarte TVs sowie Anwendungen zur Standortverfolgung oder Spionage. Angreifer werden dadurch im Alltag ihrer Ziele omnipräsent
- **Risikofaktoren**: geringere Digitalkompetenz und Abhängigkeit in der Nutzung von IT von anderen (Menschen mit Behinderung, Frauen, Senioren, Kinder), niedriger/unsicherer sozialer/ökonomischer Status (Geflüchtete, LGBTQ, Menschen mit geringem Einkommen)

Formen digitaler Gewalt im Kontext Tech Abuse

1. Toxische Inhalte (z.B. Drohungen, Beleidigungen, Einschüchterungen)
2. Content leak: Veröffentlichung sensibler privater Daten
3. Überlastung: Massenhaftes Senden von Nachrichten
4. Falsches Reporting: Missbrauch von Services zur Diskreditierung
5. Überwachung: Missbrauchs von Technologie, um Zugriff auf Kommunikation, Bewegung und sonstige Aktivitäten zu erhalten
6. Ausschluss und Kontrolle: Ausnutzen eines privilegierten Zugangs, um betroffene Person von Gerät/Account bzw. deren Steuerung fernzuhalten oder diese zu manipulieren

Vier Phasenmodell zur omnipotenten Omnipräsenz

1. Einrichtung: Kontrolle über Geräte und Benutzerkonten erlangen
2. Verdeckte Überwachung (Mitlesen von Nachrichten, Verfolgen des Browserverlaufs, Bewegungsdaten tracken etc.)
3. Offene Kontrolle: Aufstellen von Regeln z.B. Einschränkung der Kommunikation, von Freizeitaktivitäten, des sozialen Netzwerks und Kontrolle über deren Einhaltung durch Mitlesen von Nachrichten, Tracking, Geräteadministration etc. Androhen von Strafe bei Nichtbefolgung
4. Vergeltung: Bei Trennung erhöhte Wahrscheinlichkeit der Eskalation. Vom Löschen wichtiger Daten über Veröffentlichung von Inhalten, die die Reputation der betroffenen Person zerstören bis hin zu Zugriff auf das Online-Banking ist alles denkbar, was das Leben der betroffenen Person schädigt.

Missbrauchstaktiken im Bereich IoT

Taktik	Isolation	Engführung der Wahrnehmung	Überwachung	Drohungen	Degradierung	Belohnungen	DARVO (Deny Attack Reverse Victim and Offender)	Induzierte Schwäche bzw. Erschöpfung
Ziel	Von sozialer Unterstützung abschneiden, vermindert die Chancen, Hilfe zu bekommen oder den Angreifer verlassen zu können. Abhängigkeit wird erhöht (emotional, finanziell, technisch usw.) Angreifer wird zum SPOC zwischen Betroffener und Außenwelt.	Betroffene soll an ihrer Wahrnehmung und ihrem Urteilsvermögen zweifeln (erhöht die Glaubwürdigkeit des Angreifers wie auch die Abhängigkeit von ihm).	Verfolgen der Aktivitäten, prüfen, dass die Person nichts macht, was nicht im Sinne des Angreifers ist. Dient der Manipulation und der Einschränkung der Autonomie. Im Bewusstsein, überwacht zu sein, verändert die Betroffene ihr Verhalten und vermeidet Aktivitäten, die negative Konsequenzen nach sich ziehen.	Sollen der Betroffenen suggerieren, der Angreifer hat die Kontrolle.Erzeugen Angst und Verzweiflung. Kann sowohl zu physischen wie auch psychischen Beeinträchtigungen führen. Schränkt die Handlungsfähigkeit der Betroffenen ein, auf andere wirkt sie mental instabil oder sogar gestört.	Betroffene soll sich wertlos fühlen, mindert oder verhindert, dass Widerstand geleistet wird, auch im Wechselspiel mit positivem Feedback, um den Eindruck zu vermitteln, der Angreifer habe sich geändert. Kann so eingesetzt werden, dass die Betroffene sich selbst für das Verhalten des Angreifers verantwortlich hält, Selbstvertrauen wird zunehmend vom Angreifer abhängig, so dass es schwerer wird, ihn zu verlassen	Betroffene wird motiviert, sich in Situation zu fügen. Kann auch zu Unsicherheit bzgl. der wahren Natur des Angreifers führen bzw. der eigenen Gefühle ihm gegenüber.	Täter-Opfer-Umkehr: Täter vermeidet jede Übernahme von Verantwortung für sein Verhalten, Betroffener wird vorgeworfen, Verhalten selbst induziert zu haben bzw. dass die Betroffene diejenige sei, die stalkt/manipuliert/missbraucht.	Schwächt die Betroffene mental und physisch, reduziert Gegenwehr und Wahrscheinkeit des Beziehungsabbruchs
Beispiel	Überwachung der Online-Aktivitäten und digitaler Kommunikation inkl. besuchter Webseiten, Einkäufe, Postings etc. Übernahme der Kontrolle über die Online-Aktivitäten. Stehlen der Geräte oder des Online-Accounts, auch Löschen von Online-Accounts. Missbrauch smarter Türschlösser, um die Bewegungsfreiheit einzuschränken. Verfälschte Informationen online teilen, persönliche Informationen offen legen, bildbasierte Gewalt	a) Missbrauch Smartphone damit die Betroffene nur die Informationen erhält, die der Angreifer durchlassen will. Auch Beschränkung des Zugangs zu sozialen Medien, Nachrichtenportalen und anderen Kommunikationsplattformen. Erschwerter Zugang Betroffener zu Informationen zu ihren Rechten oder Unterstützung. b) Über Social Media Präsenz der Betroffenen in ihrem Namen beschämende oder rufschädigende Kommunikation verbreiten. c) Zugriff auf Smarthome-Geräte, zum Sammeln persönlicher Informationen über die Betroffene, ggfls. auch deren Manipulation. Betroffene beginnt an ihrer Wahrnehmung zu zweifeln (gaslighting)	a) Tracking der Social Media Aktivitäten, b) Ausnutzen von Smart Home Kamera, um die täglichen Aktivitäten zu verfolgen, c) Nutzen von Spyware um Kommunikation: Anrufe, E-Mails, Social Media, besuchte Webseiten, d) Nutzen von Trackern, um die Bewegung der Betroffenen nachvollziehen zu können und immer zu wissen, wo die Betroffene sich aufhält	Drohungen im Kontext Tech Abuse beinhaltet: a) Veröffentlichen von kompromittierenden Bildern oder Videos (z.B. revenge porn), b) Wenn Angreifer Zugang zum Social Media Account hat: Versenden von Hassnachrichten, um Beziehungen oder Reputation zu zerstören, c) den Zugang zu Smart Devices einschränken (Thermostat, Türschloss, TV)	Angreifer sammelt z.B. kompromittierende Informationen um die Betroffene zu erniedrigen. Smart watches, Smarte Kameras, smarte TVs können hierfür als Waffen eingesetzt werden. Andere IoT Geräte können zur Bestrafung eingesetzt werden, um z.B. Musik ein- oder auszuschalten oder die Temperatur herunterzuregeln. Auch das Einschränken der Mobilität durch Smarte Kameras oder Türschlösser kann einen degradierenden Effekt haben.	Lobende Worte in den Sozialen Medien ebenso wie Geschenke, bspw. ein neues IoT-Device, bei dessen Einrichtung der Angreifer hilft, um es später zur Kontrolle oder Degradierung einsetzen zu können.	Täter löscht Beweise. Betroffene kann nur noch auf ihr Gedächtnis zurückgreifen, an dem sie zunehmend zweifelt.	Z.B. durch ständige Anrufe/Nachrichten, die dem Opfer keine Zeit geben, zur Ruhe zu kommen. Auch Missbrauch des Zugriffs auf Smart Speaker um mitten in der Nacht laute Musik einzuschalten

Maßnahmen und nächste Schritte

Unterstützung für die Unterstützenden

- Workstream „Technische Anlaufstelle für Digitale Partnerschaftsgewalt“
- Initiiert in 2023 im Rahmen des Dialogs für Cybersicherheit (bis Oktober 2024)

Umfasst

- Bedarfsanalyse bei Beratungsstellen/Frauenhäusern
- Best Practices für Technikkompetenzzentren/Tech Clinics
- Prototyp
- Konzept

Kontakt: projekt-digitalegesellschaft@bsi.bund.de

Vernetzung fördern

- Aufbau eines Netzwerks zum Austausch von Wissen zwischen Beratungsstellen, IT-Experten, Bundesverwaltung, Wissenschaft + Forschung, aber auch Diensteanbieter und Hersteller (Sensibilisierung und non-abusive Design: Corporate Digital Responsibility)
- Einrichtung einer Verweisungsstruktur zwischen verschiedenen Initiativen im Rahmen des Cybersicherheitslotsen
- Durchführung von themenspezifischen Veranstaltungen zum Wissenstransfer wie „BSI im Dialog“ am 11. Februar 2025

Kontakt: katharina.witterhold@bsi.bund.de

Brown et al. (2024)

Design gegen Missbrauch

- Visuelle Benachrichtigungen darüber, wer Zugriff auf ein IoT Device bzw. auf die dort gespeicherten Informationen hat.
- Visuelle Benachrichtigungen darüber, mit welchem Gerät von wem und wann zuletzt auf ein IoT Device zugegriffen wurde
- Visuelle oder akustische Signale, die anzeigen, dass ein Sensor aktiv ist.
- Zugang über Webportale: Nachhalten von Information, wann und von wem der letzte Zugriff erfolgt ist. Hinweis auf Zugriff über Web auch auf dem Gerät
- Passwort-Zurücksetzen: MFA
- Interkonnektivität transparent gestalten: Verbinden sich IoT-Geräte miteinander, kann das zu unerwünschten Nebeneffekten führen. Z.B. wenn ein Fitnesstracker sich unbemerkt mit dem Smartphone verbindet und die darauf empfangenen Nachrichten reproduziert.

IT Grundschutz Personal

- Entwicklung eines Katalogs mit Maßnahmen zur Basissicherung als Ableitung aus dem IT Grundschutzkompendiums
- Rekonstruktion von Nutzerprofilen auf Grundlage der Befragung „IT-Sicherheitspraxis in Privathaushalten“
- Verständigung auf Best-Practices für das IT-Sicherheitsmanagement von Privatpersonen
- Enabling und Empowerment für Privatpersonen in diversen Lebenslagen

Kontakt: beiratdigitalerverbraucherschutz@bsi.bund.de

Das zentrale Element im Kampf gegen digitale Gewalt ist das kontinuierliche Empowerment der Betroffenen, vor, während und nach der Erfahrung von (Tech-)Missbrauch.

Referenzen und Ressourcen

https://www.bundeskanzleramt.gv.at/agenda/frauen-und-gleichstellung/gewalt-gegen-frauen/gewaltformen/gewalt-im-netz.html

https://www.frauen-gegen-gewalt.de/de/infothek/digitale-gewalt/was-ist-das.html

ETSI EG 203 936 0.0.9. Implementing Design Practices to Mitigate Consumer IoT Enabled Coercive Control:
https://www.etsi.org/deliver/etsi_tr/103900_103999/103936/01.01.01_60/tr_103936v010101p.pdf

https://antistalking.haecksen.org/

https://www.aktiv-gegen-digitale-gewalt.de/de/

Bundesverband Frauenberatungsstellen (bff) & Prasad, N. (2021): Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung. Formen und Interventionsstrategien. Transcript.

Bayerisches Forschungsinstitut für Digitale Transformation & SZ Institut (2023): bidt-Digitalbarometer international. Verfügbar online unter: https://www.bidt.digital/wp-content/uploads/sites/2/2023/09/Analysen-Studien-bidt-Digitalbarometer.international.pdf

Brown, A., Harkin, D., & Tanczer, L. (2024): Safeguarding the 'Internet of Things' (IoT) for Victim-Survivors of Domestic and Family Violence (DFV): Anticipating Exploitative Use and Encouraging Safety-by-Design. In: Violence Against Women.

Stark, Evan (2024, zuerst 2007): Coercive Control. How Men Entrap Women in Personal Life. Oxford University Press.