care digital

Organisationen sicher im digitalen Raum

inhalt

Impressum *Stand Juli 2022*

Herausgeber	Zentralwohlfahrtsstelle der Juden in Deutschland e.V. Hebelstraße 6 60318 Frankfurt am Main T 069 944371 0 E zentrale@zwst.org
Konzept und Redaktion	Laura Cazés, Regina Potomkina, Irina Rosensaft
Gestaltung	DAUBERMANN
Bildnachweise	ZWST (sofern nicht anders angegeben)

organisationen digital sicher machen. mabat unterstützt.

Irina Rosensaft, Projektleitung Digitale Transformation

Die Sozialwirtschaft, also auch die jüdische Wohlfahrtspflege und jüdische Gemeinden, erlebt im Zuge der Digitalisierung einen technologischen Umbruch, der zu einschneidenden Veränderungen führt. Das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) hat sich daher 2019 in Zusammenarbeit mit der Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege dazu entschlossen, ein Vorhaben zur Digitalen Transformation der Wohlfahrtspflege in Form eines Bundesprogramms zu Digitaler Teilhabe und gesellschaftlichem Zusammenhalt zu initiieren. 2019 wurde im Zuge dessen die Digitalisierungsinitiative der Zentralwohlfahrtsstelle der Juden in Deutschland (ZWST) „Mabat" gegründet, die seither durch das BMFSFJ gefördert wird.

„Mabat" setzt sich zum Ziel, die jüdischen Gemeinden auf dem Weg der digitalen Transformation zu begleiten und so digitale Teilhabe von Kindern und Jugendlichen, Senior:innen und Unterstützungsbedürftigen an gesellschaftlichen Prozessen zu ermöglichen. Wir unterstützen unsere Mitgliedsorganisationen beim Aufbau digitaler Infrastruktur und durch die Vermittlung digitaler Kompetenzen in allen Generationen und Sozialräumen. Des Weiteren bietet „Mabat" die Möglichkeiten, sich zu Themen rund um die Digitalisierung auszutauschen, Investitionen in digitaler Infrastruktur zu tätigen, praxisnahe Weiterbildungsmaßnahmen wahrzunehmen und somit Digitale Transformation in Organisationen strukturell anzugehen.

Die Digitalisierungsinitiative „Mabat" (hebr. „Blick") blickt gezielt in die Zukunft und will jüdische Gemeinden für die Herausforderungen disruptiver Innovation und gesellschaftlichen Wandels wappnen. Es bedeutet gleichzeitig, den Blick auch nach innen zu richten, in unsere Organisationen. Es ist ein ganzheitlicher und ein mehrdimensionaler Blick. Die ZWST versteht die digitale Transformation als eine Querschnittsaufgabe, die die Gesellschaft als Ganzes und somit auch soziale Akteur:innen in allen Arbeitsbereichen betrifft.

Digitalisierung betrifft Mitarbeiter:innen, wenn sie Dienstleistungen der Gemeinde gestalten, Prozesse verwalten oder neue Systeme und Anwendungen am Arbeitsplatz einsetzen, ehrenamtliche Führungskräfte jüdischer Gemeinden, wenn sie die Gemeinde für die nächste Generation attraktiv gestalten möchten; sie ermöglicht Vernetzung und Informationsaustausch mit Freunden in der ganzen Welt und mehr Unabhängigkeit im Alter. Der Schutz und die Sicherheit unserer Zielgruppen stehen bei allen Gestaltungsprozessen immer im Vordergrund. Digitalisierung stellt dabei besondere Herausforderungen an die Arbeit jüdischer Gemeinden dar, besonders im Hinblick auf digitale Sicherheit und Datenschutz. Mit dem Einsatz digitaler Anwendungen, mit der Verlegung unserer Angebote in digitale Räume eröffnet sich eine neue Ebene, auf der der Schutz für Gemeindemitglieder gewährleistet werden muss.

Der Schutz von Daten, Prozessen und auch der Schutz unserer Netzwerke stellt eine besondere Unsicherheit dar. Deshalb ist auch das Verständnis von Präventions- und Schutzmaßnahmen und der sichere Umgang mit IT- und Cybersystemen so elementar für die Arbeit in jüdischen Gemeinden und Organisationen.

Diese Broschüre soll den Einstieg in diese komplexe Thematik bieten und jüdischen Organisationen einen Überblick über zentrale Hinweise und niedrigschwellige Maßnahmen liefern. Sie ist eine inhaltliche Zusammenfassung der Online-Tagung „IT- und Cyber-Security: Daten, Systeme und Internetanwendungen", die von 16.–17. Juni 2021 in Kooperation mit dem Fraunhofer Institut für Sichere Informationstechnologie SIT in Darmstadt stattfand.

Bleiben Sie mit uns in Kontakt:
digitalisierung@zwst.org

Die Digitalisierungsinitiative Mabat der ZWST wird durch das Bundesministerium für Familie, Senioren, Frauen und Jugend im Rahmen des Förderprogramms „Zukunftssicherung der Freien Wohlfahrtspflege durch Digitalisierung" unterstützt.

Gefördert vom

Bundesministerium für Familie, Senioren, Frauen und Jugend

cybersecurity, it-security und informationssicherheit

IT-Sicherheit, Informations-sicherheit und Cyber-Sicherheit: Wo liegen die Unterschiede?

In den letzten Jahren haben Cyberattacken und Angriffe auf organisationsinterne IT-Systeme zugenommen – eine Kehrseite der Digitalisierung. **IT-Sicherheit, Informationssicherheit und Cyber-Sicherheit** werden daher immer wichtiger. Als Nicht-Expert:in verliert man bei den verschiedenen Begrifflichkeiten jedoch schnell den Überblick, deshalb gibt es hier eine kurze Übersicht über die Bedeutungen und Unterschiede.

IT-Sicherheit, Informations-sicherheit, Cyber-Sicherheit – keine Synonyme

Grundsätzlich ist es so, dass die drei genannten Begriffe keine festen, allgemeingültigen Definitionen haben. Ihre Verwendung hängt immer von dem Kontext und dem konkreten Zusammenhang ab, in dem sie gebraucht werden. Viele verwenden sie aber synonym, was den Eindruck erweckt, als handele es sich um ein- und denselben Sachverhalt. Allerdings gibt es einige Aspekte, die IT-Sicherheit, Informationssicherheit und Cyber-Sicherheit voneinander unterscheiden.

Was ist Informationssicherheit?

Der Begriff der Informationssicherheit bezeichnet den **Schutz von Informationen in jeglicher Form** – ob digital auf einem Datenträger oder analog auf dem Papier, ob mit Personenbezug oder ohne. „Informationen" werden in diesem Zusammenhang als „interpretierte Daten" definiert. Damit ist gemeint, dass reine Daten, wie zum Beispiel Ziffern, erst nach ihrer Interpretation zu Informationen, also zum Beispiel Uhrzeiten oder Geburtsdaten, werden.
Die Informationssicherheit hat den Schutz dieser Informationen zum Ziel und beruht dabei auf drei Bereichen: **Vertraulichkeit, Verfügbarkeit und Integrität**. Das bedeutet, dass sensible Daten vor dem unberechtigten Zugriff Dritter geschützt werden, für berechtigte Nutzer:innen aber zu jeder Zeit vollständig und richtig zugänglich sind. Dieser Schutz wird durch organisatorische Maßnahmen und klare Handlungsvorgaben im Unternehmen umgesetzt.

Was ist IT-Sicherheit im Unterschied zu Informationssicherheit?

Die IT-Sicherheit ist ein **Teilbereich der Informationssicherheit**, die sich auf die **elektronisch gespeicherten Informationen und IT-Systeme** bezieht. Insbesondere die heutzutage vermehrt digital gespeicherten und übertragenen Informationen sind vielen möglichen Bedrohungen ausgesetzt: Vom unberechtigten Zugriff Dritter auf die Daten, über Spionage und Sabotage, bis hin zu Hackerangriffen.
Das Ziel der IT-Sicherheit ist, Unternehmen und Organisationen gegen diese Bedrohungen und die Folgeschäden zu schützen. Auch hierbei greifen die drei Schutzziele **Vertraulichkeit, Verfügbarkeit und Integrität**. Die IT-Sicherheit wird ebenfalls durch organisatorische Maßnahmen und entsprechende Vorgaben in Unternehmen umgesetzt und fußt beispielsweise auf Antivirenlösungen, Firewalls und Backups.

Wie fügt sich die Cyber-Sicherheit ein?

Die sogenannte Cyber-Sicherheit bezieht sich prinzipiell auf den gleichen Bereich wie die IT-Sicherheit, wird jedoch auf den **gesamten Bereich des Internets und jeglicher Netzwerke** ausgeweitet. Da viele Daten und auch Dinge heutzutage über Netzwerke miteinander und mit dem Internet verbunden sind, kann die Sicherheit nicht mehr isoliert betrachtet werden. Das bedeutet, die Cyber-Sicherheit schließt alle **auf Netzwerken basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen** mit ein – und damit auch Infrastrukturen wie Stromversorgung oder Telekommunikation. Damit ist Cyber-Sicherheit ein Thema der Gesamtheit, das nicht nur auf die eigene Firma oder Umgebung begrenzt ist. Zahlreiche Bedrohungen und sich ständig weiterentwickelnde Cyberkriminalität in Form von Viren, Würmern, Spyware oder Trojanern erfordern umfassende und immer aktuell gehaltene Schutzmaßnahmen.

Was bedeutet das für Organisationen?

Organisationen müssen sich gegen die Gefahren und Bedrohungen, die die Digitalisierung mit sich bringt, schützen können. In der praktischen Umsetzung gibt es zahlreiche mögliche Maßnahmen, die man ergreifen kann. Sie alle sollten jedoch Teil eines umfassenden Sicherheitskonzeptes sein, das sowohl technische als auch organisatorische Maßnahmen und Handlungsrichtlinien beinhaltet. Dieses Sicherheitskonzept braucht eine gewisse Flexibilität, denn digitale Angreifer verbessern laufend ihre Strategien. Die drei Bereiche Informations-, IT- und Cyber-Sicherheit sind somit zentrale Erfolgsfaktoren für Organisationen. Wer diese Begriffe kennt und ihre Bedeutung einordnen kann, hat bereits den ersten Schritt getan. Wenn aus diesem Verständnis konkrete Handlungen für Organisationen abgeleitet werden, werden diese für die Herausforderungen der Digitalisierung gewappnet.

Blog IT-Security QR-Code1

glossar

Alle QR-Codes aus der Broschüre finden Sie zum Abscannen auf den Seiten 43 bis 45.

ADVANCED PERSISTENT THREAT *APT*
APT-Attacken zielen häufig darauf ab, Informationen zu stehlen und weniger das Netzwerk der angegriffenen Organisation zu schädigen. Das Ziel vieler APT-Angriffe ist es, dauerhaften Zugang zum Zielnetzwerk zu erlangen und aufrechtzuerhalten und nicht, so schnell wie möglich hinein- und hinauszukommen.
QR-Code 2

BACKUP
Mit einem Backup lassen sich Daten auf einem geeigneten Speichermedium (z.B. einer externen Festplatte) sichern. Am Ende eines Backups steht eine Sicherheitskopie zur Verfügung, die wichtige Daten in sogenannter redundanter Form enthält, also als Dopplung. Werden alte Daten benötigt oder gibt es einen plötzlichen Datenverlust, lässt sich über das Backup der Datenbestand ganz oder teilweise wiederherstellen. Dies kann durch manuelle Methoden (z.B. Zurückkopieren einzelner Dateien) oder durch spezielle Backup-Software mit Restore-Funktionen erfolgen. QR-Code 3

CLOUD / CLOUD-DIENSTE
Unter Clouds kann man sich (große) Rechenzentren vorstellen, die mit dem Internet verbunden sind. Dort werden verschiedene Dienste für den Privatanwender und für Unternehmen angeboten. Der Cloud-Anbieter betreibt diese Rechenzentren hoch automatisiert, sodass er sehr vielen Benutzern gleichzeitig seine Dienste anbieten und sehr hohe Anforderungen bewältigen kann. Dies gelingt auch deshalb, weil er standardisierte Dienste anbietet, die für alle erst mal gleich sind. Wenn wir einen Cloud-Dienst nutzen, lagern wir private und schützenswerte Daten an den Cloud-Provider aus. Wir geben dabei Kontrolle und Verantwortung ab und müssen uns darauf verlassen, dass unsere Daten ausreichend geschützt werden. QR-Code 4

CONTENT MANAGEMENT SYSTEM *CMS*
Ein CMS ist eine Software, die zur Erstellung und Verwaltung von Inhalten – in Text-, Bild-, Video- oder sonstiger Form – verwendet wird. CMS werden vor allem zum Betreiben von Websites eingesetzt. QR-Code 5

CREDENTIALS
Credentials sind Ausweispapiere, Berechtigungsnachweise, Zeugnisse oder Legitimationen in Form von Daten, die einem System die Identität eines anderen Systems oder von Benutzer:innen bestätigen sollen. QR-Code 6

CYBERKRIMINALITÄT
Cyberkriminalität bezieht sich auf alle illegalen Aktivitäten, die mithilfe von Computern oder dem Internet durchgeführt werden. Cyberkriminelle – von skrupellosen Einzelpersonen über organisierte kriminelle Gruppen bis hin zu staatlich geförderten Gruppen – nutzen verschiedene digitale Techniken für ihre Cyberangriffe. QR-Code 7

DARKNET
Das Darknet ist ein versteckter Teil des Internets – unsichtbar für alle, die mit einem Standard-Browser unterwegs sind. Während Kommunikation im „offenen" Internet zurückverfolgbar ist, bleibt man im Darknet anonym. Dies bietet Kriminellen eine Plattform, um illegale Dienstleistungen und Güter anzubieten oder verbotene Inhalte jederart zu teilen oder zu erwerben. QR-Code 8

DEEP FAKES
Deep Fakes sind täuschend echt wirkende, manipulierte Bild-, Audio- oder auch Videoaufnahmen. Sie werden mit Programmen, Apps und der entsprechenden Software mit Hilfe von künstlicher Intelligenz erzeugt. In Echtzeit lassen sich Gesichter und Stimmen tauschen, Personen damit in einem anderen Kontext darstellen. Menschen sagen Dinge, die sie nie gesagt haben oder vollziehen Handlungen, die nie stattgefunden haben. Deep Fakes können eine große Gefahr für die Gesellschaft und Politik darstellen. Insbesondere dann, wenn sie genutzt werden, um die öffentliche Meinung zu manipulieren und politische Prozesse gezielt zu beeinflussen. QR-Code 9

DENIAL-OF-SERVICE *DOS*
Denial of Service – oder kurz DoS – bedeutet so viel wie etwas unzugänglich machen oder außer Betrieb setzen. Technisch passiert dabei folgendes: Bei DoS-Attacken wird ein Server gezielt mit so vielen Anfragen bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht. QR-Code 10

DOXXING
Der Begriff „doxxing“ stammt vom verkürzten Begriff „doxs“ für das englische Wort „documents“ (Dokumente). Doxxing (oder Doxing) ist die Praxis, die sensiblen persönlichen Informationen einer Person aufzudecken und online öffentlich zu machen. Hacker verwenden Doxxing, um jemanden online zu belästigen, zu bedrohen oder sich an ihm zu rächen. QR-Code 11

EXE-DATEI
Die Abkürzung und Datei-Endung „exe“ steht für den englischen Begriff „executable“ („ausführbar“). Beim Öffnen solch einer Datei wird somit eine bestimmte Aktion ausgeführt. In der Regel bezieht sich dies auf den Start eines Programms. Für erfahrene Programmierer ist es problemlos möglich, innerhalb einer Exe-Datei auch Schadsoftware zu verstecken. QR-Code 12

HACKER
Hacker sind technisch versierte Personen im Hard- und Softwareumfeld. Sie finden Schwachstellen von Systemen, um auf sie aufmerksam zu machen oder sie für bestimmte Zwecke wie unbefugtes Eindringen oder zur Veränderung von Funktionen zu nutzen. QR-Code 13

HOST PROVIDER
Beim Host Provider handelt es sich um einen externen Server, der in einem Computernetzwerk integriert ist. Er bietet Programm-, Informations- und Rechner-Ressourcen sowie die Infrastruktur und das Management für das Webhosting gegen Bezahlung an. QR-Code 14

IP-ADRESSE
Eine IP-Adresse ist eine individuelle Adresse, die ein Gerät im Internet oder auf einem lokalen Netzwerk identifiziert. IP steht für „Internetprotokoll“, wobei es sich um einen Satz von Regeln handelt, der das Format der Daten bestimmt, die über das Internet oder das lokale Netzwerk gesendet werden. QR-Code 15

MALWARE
Malware ist ein Überbegriff für jede Art von „bösartiger Software“, die entwickelt wurde, um ein Gerät ohne das Wissen von Nutzer:innen zu infiltrieren. Es gibt viele Arten von Malware, und jede geht anders vor, um ihr Ziel zu erreichen. Alle Malware-Varianten haben jedoch zwei entscheidende Merkmale gemeinsam: Sie sind heimtückisch und zielen darauf ab, Schaden zufügen. QR-Code 16

PATCH
Patch (dt. Flicken) bezeichnet ein Software-Update für bestehende Anwendungen oder Betriebssysteme zur Behebung von Fehlern oder Sicherheitslücken.
QR-Code 17

PHISHING
Phishing beschreibt den Versuch des Diebstahls von Kennungen und Passwörtern per Internet durch den Versand von gefälschten E-Mails oder SMS. Internet-Anwender:innen werden von Cyberkriminellen mittels täuschend echt nachgemachter E-Mails auf gefälschte Internetseiten von Banken, Onlineshops oder anderen Onlinediensten gelockt, um dort deren Benutzerkennungen und Passwörter zu ergattern. Die ergaunerten Daten werden beispielsweise für Kontoplünderungen oder Hackerangriffe auf Unternehmen verwendet.
QR-Code 18

RANSOMWARE
Ransom ist der englische Begriff für „Lösegeld“. Bei Ransomware handelt es sich um Erpressungssoftware, die Ihren Computer sperren kann und anschließend ein Lösegeld für die Freigabe fordert.
QR-Code 19

SCRIPT
Ein Computerskript ist eine Liste mit Befehlen, die von einem bestimmten Programm oder einer Skripting-Maschine ausgeführt werden. Skripte können verwendet werden, um Prozesse auf einem lokalen Computer zu automatisieren oder um Webseiten im Internet zu generieren und darzustellen.
QR-Code 20

SILENCING
Silencing (dt. Verstummen) bedeutet, dass sich Internetnutzer:innen aus Angst vor Hasskommentaren und heftigen Hassreaktionen seltener zu ihrer politischen Meinung / Einstellung bekennen. Folglich reduziert sich die Meinungsvielfalt im Netz, wodurch auch das gesellschaftliche Meinungsbild verzerrt wird.
QR-Code 21

TRACKING / WEBTRACKING
Das Wort Tracking kommt aus dem Englischen und bedeutet auf Deutsch „Verfolgung“. Dabei wird im Internet eine Art Spur eines Nutzers verfolgt. Viele Webseiten zeichnen das Nutzerverhalten im Internet mit Hilfe von Trackingdiensten auf. Zur Überwachung zählen Datensätze wie Zeitpunkt, Bewegungen innerhalb der Seite und von wo ein User auf die Webseite gekommen ist, zum Beispiel über eine Suchmaschine oder über Werbeeinblendungen.
QR-Code 22

WEBANALYSE TOOLS
Webanalyse-Tools dienen der Überprüfung des Besucherverhaltens einer Website. Sie sind das Mittel der Webanalyse und sollen die komplexen Daten, die von Servern und Clients gesammelt werden, grafisch sichtbar machen.
QR-Code 23

WORDPRESS
WordPress ist ein frei verfügbares Content Management System, mit dem sich Webseiten gestalten und verwalten lassen.
QR-Code 24

online-bedrohungen und it-sicherheit der internet-infrastruktur deutschlands

Fraunhofer SIT

Prof. Dr. Shulman wurde vielfach für ihre Forschung ausgezeichnet, zuletzt mit dem 8. Deutschen IT Security Award für innovative Lösungen zur Verbesserung der Internetsicherheit und gilt als Koryphäe auf dem Gebiet der Netzwerk- und Computersicherheit. Sie ist seit Februar 2022 Professorin im Fachbereich Informatik an der Johann Wolfgang Goethe-Universität Frankfurt am Main und hat eine LOEWE-Spitzen-Professur inne.

Prof. Dr. Haya Shulman

Direktorin der Abteilung Cybersecurity Analytics and Defences am Fraunhofer Institut für Sichere Informationstechnologie SIT

Prof. Dr. Haya Shulman

Alles, was digitalisiert ist, kann angegriffen werden

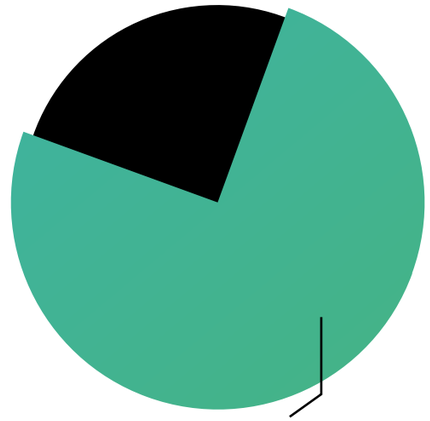
Die ganze Gesellschaft ist digitalisiert: Rechenzentren, Medien, Banken, Gesundheitsvorsorge, soziale Netzwerke, öffentliche Sicherheit, Polizei, Verteigung, Stromkraftwerke, Wasserversorgung, beinahe alles ist digitalisiert – **und alles, was digitalisiert ist, kann auch angegriffen werden.**

Cyberangriffe gefährden die gesamte Gesellschaft und können sogar Menschenleben kosten

Die Gefahr, dass Firmen und Unternehmen angegriffen werden können, ist hoch. Die zunehmende Anzahl der Angriffe führt dazu, dass große Versicherungsunternehmen wie AXA nicht mehr gegen Cyberangriffe versichern. Gleichzeitig verursachen Cyberangriffe großen Schaden für die Gesellschaft und Wirtschaft: Es gibt Schätzungen von Bitkom, dass in der **Wirtschaft rund 100 Milliarden Euro Schaden pro Jahr entstehen. 3 von 4 Fällen sind Opfer von Sabotage oder Spionage.** Über den immensen wirtschaftlichen Schaden hinaus werden Menschenleben riskiert: So musste die Uniklinik in Düsseldorf in der Ambulanz eine schwerkranke Patientin abweisen, weil **HACKER** die IT-Infrastruktur der Klinik lahmgelegt hatten.

Wirtschaftlicher Schaden durch Cyberangriffe

Rund 100 Mrd. € pro Jahr

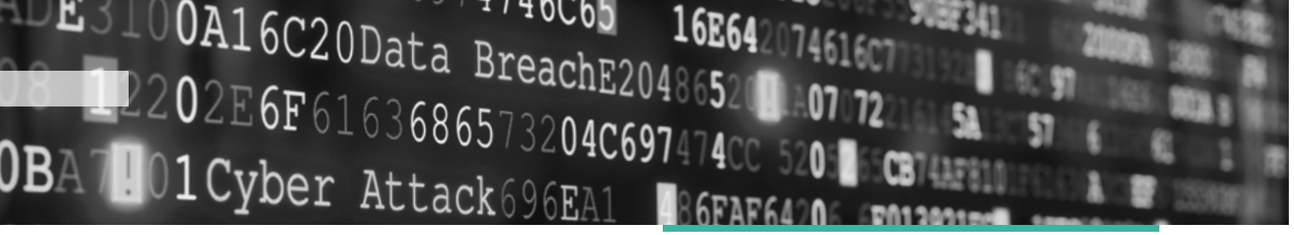


75 Mrd.

Euro davon verursacht durch Sabotage oder Spionage

Beispiele für die Zunahme von Cyberangriffen

> Eine finnische Klinik für Psychotherapie mit 40.000 Patient:innen wurde mit **RANSOMWARE** angegriffen. Cyberkriminelle haben vertrauliche Gespräche der Patient:innen mit ihren Therapeut:innen gestohlen und Lösegeld von der Klinik gefordert. Auch einzelne Patient:innen erhielten Lösegeldforderungen über E-Mail. > Daten der Colonial Pipeline der USA wurden gestohlen und die Systeme mit Erpressungssoftware gesperrt. Nach dem Angriff wurde das gesamte Rohr-Leitungsnetz von Texas bis New York stillgelegt, was zu Benzin-Versorgungsengpässen führte. Der Betreiber hat zugegeben, ein Lösegeld von 75 Bitcoin bezahlt zu haben, das entspricht über 3 Millionen Euro. > Auch in Deutschland passieren solche Fälle: Durch einen Cyber-Angriff wurde ein Supermarkt in Hessen gehackt und die Datennetze abgeschaltet. Im Darknet wurden Kundendaten veröffentlicht, um den Supermarkt zu erpressen. Politiker, Forschungseinrichtungen und Universitäten in Deutschland sind ebenfalls betroffen.



Wer sind die Angreifer und woher kommen sie?
Deutschland ist im Visier, da es ein wichtiges Ziel in Europa ist. Hauptsächlich kommen die Angreifer aus drei Ländern: **Russland**, **China** und **Iran**. Dabei handelt es sich um politisch motivierte Angriffe. > Russland hat politische Spionage und Desinformation zum Ziel. > China ist wirtschaftlich orientiert: Zu den Zielen gehören alle Sektoren, die für den Fünfjahresplan der Entwicklung Chinas von Interesse sind.

> Iran ist politisch motiviert: Ziele sind Behörden, Ministerien und Militär. Die Angreifer sind **CYBERKRIMINELLE**, die entweder einen finanziellen Vorteil suchen oder sehr gut organisierte **APT-GRUPPEN**, die als regierungsnah eingestuft werden können und den Staat, der sie beauftragt, unterstützen. Es gibt Dutzende bekannte APT-Gruppen, die bekannte Vorgehensmuster und Ziele haben.

Was sind die Ziele von Cyberkriminellen?

> Spionage
Dadurch will man strategische Vorteile erlangen und den Gegner erpressen.

> Sabotage
D. h. die Behinderung von Diensten und Informationsverbreitung. Dazu zählen sogenannte **DENIAL-OF-SERVICE ANGRIFFE**.

> Desinformation
Man verbreitet falsche Informationen, die das Opfer verunglimpfen. Für politische Organisationen ist dies ein sehr wichtiges Thema, besonders vor Wahlen.

> Angriffe auf die Mediensicherheit
Verbreitung von Falschinformationen, Fake News, Manipulation, Erzeugung von gefälschten Bildern, Audios und Videos. Dies wird als **DEEP FAKES** bezeichnet.

Prof. Dr. Haya Shulman

Was sind die Einfallstore der Cyberkriminellen in der Praxis?

Gefälschte E-Mails: PHISHING

Über 40% der Server erlauben unverschlüsselt Zugriff auf E-Mails, d. h. sie können gefälschte E-Mails nicht filtern oder blockieren und akzeptieren sie. Wenn die Nutzer:innen den Betrugsversuch nicht bemerken und etwas herunterladen, werden ihre Systeme infiziert. Phishing E-Mails verbreiten sogenannte **MALWARE**. Die Gefahr verbirgt sich in ausführbaren Dateien wie **.EXE-DATEIEN**, aber auch PDFs können gefährlich sein, da sie schädlichen Code beinhalten können oder programmierbar sind. Sogar im JPEG-Bildformat lässt sich Malware verstecken. E-Mail-Adressen der meisten Organisationen sind öffentlich und daher für solche Angriffe zugänglich.

Einbruch in Internetserver

Cyberkriminelle nutzen Schwachstellen im Server, die vom Internet erreichbar sind. So z. B. bereits über eine Sicherheitslücke im Microsoft Exchange Server geschehen, wodurch in die Systeme diverser Unternehmen eingedrungen wurde. Solche Angriffe sind möglich, wenn der Server nicht **GEPATCHT** ist, ein veraltetes Betriebssystem hat oder alte Software verwendet. Auf vielen Webservern wird **WORDPRESS** verwendet, das sehr viele Schwachstellen hat. Auch Dienstleister wie **CLOUD-ANBIETER**, Rechenzentren und Lieferketten sind vor solchen Cyberattacken nicht gefeit.

Webseiten, die aufgesetzt werden, um Malware zu verbreiten

Solche Webseiten werden aufgesetzt, um Nutzer:innen zu infizieren. Man denkt, dass Webseiten nichts tun können, sobald man seinen Browser schließt oder das Netz wechselt, doch das ist falsch. Infizierte Webseiten können mit dem externen Angreifer kommunizieren, Credentials offenlegen und sogar Zwei-Faktor-Authentifizierung angreifen. Selbst wenn man die infizierte Webseite verlässt, können die schädlichen **SCRIPTS** beliebig lange im Browser bleiben und kontrolliert werden. Diese Scripts wieder zu entfernen, ist sehr schwierig.

Erbeutung von Nutzer-CREDENTIALS

Es gibt mehr als 23.000 kompromittierte Datenbanken. Viele von diesen Nutzer:innen-Accounts stammen von Einbrüchen in IT-Systeme. Diese Zugangsdaten können verwenden werden, um sich in der Bank einzuloggen, die Kreditkartennummer oder andere private Daten zu finden. Man könnte damit auch Cyberangriffe durchführen. Cyberkriminelle versuchen die gestohlenen Credentials in verschiedenen Diensten zu verwenden und sich so Zugang zu diesen zu verschaffen. Die Credentials werden im **DARKNET** verkauft oder im Internet veröffentlicht.

Was kann man tun, um Cybergefahren entgegenzuwirken?

Mitarbeiter:innen-Trainings

Mitarbeitende zu sensibilisieren und ihnen Trainings anzubieten, ist essentiell. Malware bereits richtig zu erkennen, vorsichtig mit verdächtigen oder unbekannten E-Mails und Dateien umzugehen und sie nicht direkt zu öffnen, kann viele Angriffe verhindern.

Tools zur Schwachstellenerkennung in Systemen nutzen, Lücken in Betriebssystemen patchen und das Netz vorbereiten

Ganz wichtig ist: Das Netz muss gut segmentiert und mit einer Firewall ausgestattet sein. Wenn das Netz nicht gut segmentiert ist, kann sich Malware überall verbreiten und viele Server betreffen. Wenn das Netz hingegen segmentiert ist, kann sich die Malware nicht überall verbreiten und wird zwar womöglich einen Bereich angreifen, aber dort auch bleiben. Diese Maßnahme erlaubt es, die Systeme schnell zu säubern und das Netz wieder hochzufahren. Ebenso wichtig sind **BACKUPS**, die in einem separaten Netz gespeichert und regelmäßig aktualisiert werden. Je nach Art der Daten kann die Aktualisierung bereits wöchentlich notwendig sein, um immer den aktuellen Stand sicherzustellen.

Sicherheits-Monitoring

Organisationen wird empfohlen einen Rechner aufzusetzen, der vom Netz getrennt ist und dorthin Dateien zu verschieben, die wie **PHISHING** aussehen oder verdächtig sind und diese nur dort aufzumachen.

Vorbereitung für den Ernstfall

Ein Angriff wird passieren, egal, was man tut. Das heißt, man muss für den Ernstfall vorbereitet sein und folgende Grundsatzfragen beantworten: > Wer ist wofür verantwortlich, sobald Sie betroffen sind? Es wird dringend empfohlen, eine Liste von Verantwortlichen für jede Aufgabe zu haben, da ansonsten Chaos und Ratlosigkeit herrschen. Außerdem ist es wichtig festzulegen, wen man bei einem Vorfall kontaktieren wird, zum Beispiel das Bundeskriminalamt. Kundendaten müssen besonders gesichert werden, da ansonsten je nach Art der Daten Strafverfolgung droht, falls sie öffentlich werden. > Welche IBAN verwendet man bei einem Cyberangriff? > Welche Telefonie? > Wer wird mit wem kommunizieren? Für den Fall eines Angriffs, müssen alternative Kommunikations- und Zahlungskanäle aufgesetzt werden, die funktionieren werden, wenn die Organisation gehackt wird. Wenn man diese grundlegenden Problematiken frühzeitig durchdacht hat, ist man für Cyberangriffe vorbereitet.

dsgvo – richtlinien und herausforderungen für organisationen

Dr. Barbara Sommer, Rechtsanwältin, befasst sich im Speziellen mit IT-Recht und Datenschutzrecht: Sie ist Partnerin der Kanzlei Weitnauer, die an den vier Standorten Berlin, München, Hamburg und Mannheim in Deutschland tätig ist. Darüber hinaus hat sie einen Lehrauftrag an einer Hochschule, an der sie IT-Recht für Wirtschaftsinformatiker:innen unterrichtet.

Dr. Barbara Sommer

Rechtsanwältin für IT-Recht, Datenschutzrecht und Verbraucherschutzrecht

Dr. Barbara Sommer

Was ist die DSGVO?

Die Datenschutz-Grundverordnung der Europäischen Union (EU), regelt die Verarbeitung von personenbezogenen Daten natürlicher Personen durch natürliche Personen, Unternehmen oder Organisationen in der EU.

QR-Code 25

7 allgemeine Grundsätze der EU-DSGVO

1 **Grundsätze für die Verarbeitung personenbezogener Daten**
Art. 5 DSGVO (siehe unten nachfolgend)

2 **Rechtmäßigkeit der Verarbeitung personenbezogener Daten**
Art. 6 DSGVO

3 **Bedingungen für die Einwilligung**
Art. 7 DSGVO

4 **Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft**
Art. 8 DSGVO

5 **Verarbeitung besonderer Kategorien personenbezogener Daten**
Art. 9 DSGVO

6 **Verarbeitung von personenbezogener Daten über strafrechtliche Verfolgung**
Art. 10 DSGVO

7 **Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist**
Art. 11 DSGVO

Artikel 5 DSGVO

7 Grundsätze, die sich mit der Verarbeitung personenbezogener Daten befassen:

1 **Treu und Glauben, Rechtmäßigkeit, Transparenz**

2 **Zweckbindung**

3 **Datenminimierung**

4 **Richtigkeit**

5 **Speicherbegrenzung**

6 **Integrität und Vertraulichkeit**

7 **Rechenschaftspflicht**

QR-Code 26

personenbezogene daten

Was ist laut DSGVO datenschutzkonform und wie geht man richtig mit personenbezogenen Daten um?
Im Zuge der schnellen technischen Veränderungen ist Rechtssicherheit in Bezug auf den Datenschutz kompliziert. Bis ein Gesetz umgesetzt ist, ist die Technologie häufig schon weiter. Deshalb ist es in Bezug auf das Internet und die Digitalisierung auch so schwer, gute Gesetze zu machen. Beim Datenschutz geht es vor allem um das Verständnis einiger Grundprinzipien. Wenn man diese verinnerlicht, ist ein sicherer Umgang mit Daten gar nicht mehr so schwer. Die Vermittlung einiger Grundlagen kann hier Ängste nehmen.

Oberster Grundsatz für die Datenverarbeitung: Keine personenbezogenen Daten verarbeiten, wenn es keine Rechtsgrundlage gibt.
Der Grundsatz, den Sie sich merken sollten, ist im Prinzip: **Die Verarbeitung personenbezogener Daten unterliegt einem Verbot mit Erlaubnisvorbehalt.** Sie dürfen keine personenbezogenen Daten verarbeiten, wenn Sie keine Rechtsgrundlage haben. Das ist der Grundsatz Nummer eins, den Sie immer bedenken müssen. Also immer in dem Moment, in dem Sie Daten verarbeiten, müssen Sie sich die Frage stellen: „Gibt es dafür eine Rechtsgrundlage?"

Was sind personenbezogene Daten?
Das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Laut DSGVO fallen auch Pseudonyme unter personenbezogene Daten. Das heißt es reicht z. B., dass Sie eine Nutzer-ID haben. Die IP-Adresse eines Websitebesuchers z. B., die bei jedem Aufruf einer Website zwangsläufig an deren Server übermittelt wird, gilt in Deutschland als personenbezogenes Datum. Dieser Aspekt ist in Bezug auf **ANALYSE-TOOLS** und der Einbindung von Social Media-Schnittstellen auf Webseiten wichtig.

Für Website-Betreiber gibt es besondere Kategorien personenbezogener Daten (diese Daten gibt es nicht nur für Website-Betreiber!)
Noch strengeren Anforderungen unterliegt die Verarbeitung von besonderen Kategorien personenbezogener Daten. Dies sind z. B. die ethnische Herkunft, politische Meinung, religiöse, weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit etc. Die bloße Herkunft (z. B. aus welchem Land oder welcher Stadt man kommt) ist kein sensitives Datum. Bei diesen besonderen Kategorien personenbezogener Daten gibt es gesonderte Rechtsgrundlagen.

Anwendungsbeispiel:
Braucht eine Webseite meinen Namen, um mich zu erkennen?
Sie kennen das, oder? Sie sitzen am Computer, schauen in der Suchmaschine nach einer Waschmaschine, schauen Sie sich noch ein paar Webseiten an, nehmen Ihr Handy in die Hand und sehen nur noch Waschmaschinen. Man fragt sich: „Kann mein Handy hellsehen?" Nein, Ihre Spuren im Netz werden verfolgt. Sie werden zum Subjekt einer Webseite, die weit übergreifendes **TRACKING** verwendet. Das sind im Prinzip gängige, standardisierte Technologien, die es heute gibt. Für denjenigen, der solche Tracking-Tools nutzt oder hierdurch gezielt Werbung schaltet, ist nicht wichtig, wie der getrackte Nutzer heißt. Wichtig ist nur, dass er immer wieder erreicht wird und ggf. sogar ein Profil über seine Interessen gebildet werden kann. Daher werden vom Schutz der DSGVO auch Pseudonyme erfasst.

einwilligung

Einwilligungen zur Datenverarbeitung: Wann sind sie wirklich nötig?
Häufig werden Einwilligungen auch da eingeholt, wo sie nicht nötig sind. Man sollte das auch deswegen nicht machen, weil eine Einwilligung immer frei widerrufbar ist.

Für Körperschaften des öffentlichen Rechts sind auch die Regelungen des Bundesdatenschutzgesetzes zu beachten.

Die Mitgliedsstaaten der EU durften in gewissem Rahmen eigene Datenschutzgesetze erlassen. Es gab einige sogenannte Öffnungsklauseln, bezüglich denen die DSGVO sagt, dass die Mitgliedsstaaten sie selbst regeln müssen oder dürfen. Deswegen gibt es in Deutschland zum Beispiel auch das **Bundesdatenschutzgesetz** oder Landesdatenschutzgesetze.

Anwendungsbeispiel:
Einwilligungen
Sie bestellen etwas im Internet. Der Onlineshop braucht natürlich Ihren Namen, Ihre Adresse und Ihre Zahlungsdaten, denn sonst kann er Ihnen keine Waren schicken und keine Abrechnung vornehmen. Würde er sagen, Sie müssten einwilligen und Sie würden Ihre Einwilligung mittendrin widerrufen, dann müsste er die Daten löschen und könnte die Ware nicht zusenden, also den Vertrag erfüllen. Deshalb sollte immer geprüft werden, ob es eine Rechtsgrundlage gibt. Ein Verein darf z. B. auch ohne Einwilligung Daten erheben, die für den Beitritt der Mitglieder zu der Gemeinde erforderlich sind. Wichtig ist, dass z. B. bei einem Mitgliedsantrag auch wirklich nur die Daten abgefragt werden, die erforderlich sind. Das ist im Falle einer Gemeinde nicht einfach abzuwägen. Will die Gemeinde darüber hinaus Daten erheben, an denen sie ein berechtigtes Interesse hat, so ist eine Abwägung mit den Grundrechten und Interessen der Betroffenen, also denjenigen, deren Daten verarbeitet werden, vorzunehmen.

datenverarbeitung und informationspflicht

Was bedeutet „Verarbeitung" von personenbezogenen Daten?

Verarbeitung von personenbezogenen Daten

- > Erheben
- > Speichern
- > Löschen
- > Verändern
- > Übermitteln an andere
- > Veröffentlichen (Internet, Printmedien)
- > Anonymisieren

Vorsicht bei sog. Art. 9-Daten

Bei den oben schon erwähnten besonderen Kategorien personenbezogener Daten ist eine Datenverarbeitung nur zulässig, wenn eine Rechtsgrundlage vorliegt und die weiteren Voraussetzungen des Art. 9 DSGVO vorliegen. Die kann z. B. der Fall sein, wenn die Verarbeitung auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.

Jede Einwilligung unterliegt der Beweispflicht

Viele denken, eine Einwilligung sei nur wirksam, wenn sie schriftlich abgegeben wurde. Das ist zwar nicht so, aber da derjenige, der seine Verarbeitung auf eine Einwilligung stützt, beweisen muss, dass sie auch wirklich vorliegt, sollte man diese immer schriftlich bzw. elektronisch dokumentiert einholen.

Betroffene müssen über alle Details und Risiken der Verarbeitung oder Veröffentlichung ihrer Daten informiert werden

Es reicht nicht eine Einwilligung einzuholen, dabei einfach nur zu sagen: „Sind Sie einverstanden, dass ich das im Internet poste?", sondern dem Menschen müssen die Konsequenzen mitgeteilt werden. Es ist wichtig, dass die Information komplett ist. Was wollen Sie veröffentlichen, verarbeiten und in welcher Form? Wo wird es sein? Denn was im Internet ist, bleibt. Und das kann man einfach nicht verhindern, auch weil es Archivierungsdienste für Webseiten gibt. Auch kann im Internet alles ganz einfach kopiert und weiterverbreitet werden. Aus diesem Grund muss genau informiert werden, damit die Leute sich der Risiken bewusst sind, wenn sie solch eine Einwilligung geben.

Einwilligungen sind jederzeit widerrufbar

Man muss immer darauf hinweisen, wenn man eine Einwilligung abfragt, dass derjenige die Einwilligung mit Wirkung für die Zukunft jederzeit widerrufen kann. Und die Einwilligung muss natürlich freiwillig sein. Man darf nicht unter Druck setzen oder mit Nachteilen drohen, wenn man eine Einwilligung einholt.

Wann muss ich informieren?

Je nach dem, was für ein Träger man ist, muss man sich rückversichern, ob weitere Pflichten nach dem Bundesdatenschutzgesetz oder nach Landesdatenschutzgesetz gelten. Die Rechte zur Datenverarbeitung können auch eingeschränkt sein. Bei öffentlichen Stellen gibt es z. B. zum Teil Einschränkungen des Auskunftsrechts. > Sehr wichtig ist die Pflicht nach **Artikel 13** und **14 DSGVO** **(DSGVO-Artikel: QR-Code 27)**, die jeweils einen Katalog der zur Verfügung stellenden Informationen enthalten. **Alle dort genannten Informationen müssen den Betroffenen zum Zeitpunkt der Erhebung ihrer Daten mitgeteilt werden.**

> Der **Artikel 13** regelt, was man für Informationspflichten hat, wenn man die Daten direkt vom Betroffenen erhebt. > Der **Artikel 14 r**egelt den Fall, wenn man die Daten von Dritten erhält, also was man zu tun hat, wo man etwas anzugeben hat und auf welchem Wege, wenn man die Daten von jemand anderem bekommen hat: Bei einer Übermittlung von einer Gemeinde zur anderen, zum Beispiel (sofern diese Übermittlung überhaupt zulässig ist). Das Entgegennehmen eines ausgefüllten Mitgliedsantrags ist so ein Zeitpunkt einer Datenerhebung. Daher muss dem / der Antragsteller:in auch zu diesem Zeitpunkt – in Papier oder online – die Information nach Art. 13 DSGVO vorliegen.

Man kennt den Begriff Datenschutzerklärung aus dem Internet schon lange. Aber seit Einführung der DSGVO braucht man im Prinzip immer eine Datenschutzerklärung, egal ob online oder offline, wenn man personenbezogene Daten erhebt, also gegenüber Mitgliedern, gegenüber Ehrenamtlichen usw.

Für Vertragspartner, die juristische Personen sind, gilt zwar die DSGVO nicht, aber sie haben ja in der Regel mit natürlichen Personen zu tun. Also muss man auch die Ansprechpartner:innen informieren oder ansonsten vielleicht auch Personen, für die man tätig ist und deren Daten, personenbezogene Daten, die man auch erhebt, wenn man zum Beispiel karitativ tätig ist. Zeitpunkt für die Information ist die Erhebung der Daten.

Wie muss die Person informiert werden?
Es muss gewährleistet sein, dass die Person Zugriff auf die Information hat. Wenn Sie sie zu sich in eine Geschäftsstelle bitten und der- oder diejenige unterschreibt vor Ort einen Papierantrag, kann er / sie nicht auf die Website verwiesen werden, sondern die Datenschutzerklärung sollte mit vorgelegt werden. Die Informationen müssen verständlich, transparent und natürlich richtig sein. Viele schreiben mehr in die Datenschutzerklärung, als sie tatsächlich verarbeiten, nach dem Motto: Lieber zu viel als zu wenig. Dann ist die Datenschutzinformation aber nicht mehr korrekt.

Wo dürfen die Daten abgelegt werden?
Häufig besteht Zurückhaltung bei der Nutzung von **CLOUDDIENSTEN**, aus Sorge, dass die Nutzung von externen Anbietern nicht datenschutzkonform ist. Manche speichern Daten gar auf ihren privaten Rechnern, weil sie denken, man dürfe sie nicht in der Cloud ablegen. Schon das alte Bundesdatenschutzgesetz und jetzt auch die DSGVO haben die Nutzung solcher Anbieter aber explizit über die sog. Auftragsverarbeitung geregelt. Wichtig ist, dass man mit den Anbietern einen Vertrag nach Art. 28 DSGVO schließt. Sie müssen weisungsgebunden sein und dürfen kein eigenes Interesse an den Daten haben. Vorsicht aber bei Anbietern, die Daten außerhalb der EU verarbeiten. Hier sind noch weitere Anforderungen einzuhalten.

Um Daten-Integrität zu wahren, sollten Daten niemals lokal, sondern immer zentral gespeichert werden. Man denkt immer, die Daten liegen sicherer auf dem eigenen Rechner. Aber die Frage ist: Wie gut haben Sie Ihren Rechner gesichert? Wie gut haben Sie Festplatten in Büroräumen gesichert? Wenn Ehrenamtliche vielleicht Zuhause nochmal Daten verarbeiten, haben Sie gar keine Zugriffsmöglichkeit als Organisation. Im Prinzip liegen sie in der Cloud besser, weil dann der Zugriff durch die Organisation sichergestellt ist – anders, als es auf dem Gerät eines Einzelnen ist. Und zum anderen: In Bezug auf die Sicherheit ist man auch verpflichtet, Daten-Integrität zu wahren. Das heißt, man haftet auch dafür, wenn Daten schlicht gelöscht werden oder verschwinden.

Wie werden Daten sicher gespeichert?
Bei Datenverarbeitung unter Berufsgeheimnis gelten strengere Anforderungen als üblich.
Hierfür gibt es auch spezielle Cloud-Anbieter. Bei diesen werden Daten entweder so verschlüsselt abgelegt, dass selbst der Cloud-Anbieter niemals in diese Daten reinschauen könnte oder es werden von dessen Mitarbeitern Verschwiegenheitserklärungen unterzeichnet. Die technisch-organisatorischen Maßnahmen muss man auch von allen Dienstleistern anfordern. Wenn man sich entschließt, einen Cloud Service zu nutzen oder man eine Website betreibt, liegt diese nunmal bei einem **HOST PROVIDER**.

Dann muss man sich im Zuge der Auftrags-Kontrolle zeigen lassen, ob der Anbieter die technisch-organisatorischen Maßnahmen einhält, die jeden Zugriff auf personenbezogene Daten verhindern.

Daten dürfen nicht ohne Weiteres von einer Stelle an eine beliebige andere übermittelt werden

Daten dürfen nicht so einfach von einer Stelle zur anderen übermittelt werden. Jede Übermittlung von einem Verantwortlichen an einen anderen (z. B. eine Körperschaft an einen Verein) braucht eine Rechtsgrundlage. Eine Ausnahme gilt eben nur für die Auftragsverarbeitung. Wie bereits erwähnt, kommen weitere Anforderungen hinzu, wenn die andere Stelle – egal ob Verantwortlicher oder Auftragsverarbeiter – außerhalb der EU bzw. des EWR seinen Sitz hat oder dort Daten verarbeitet. Bei US-Anbietern z.B. kann man sich seit einer Entscheidung des Europäischen Gerichtshofs aus 2019 nicht mehr auf das von diesem gekippte Privacy Shield berufen.

Verfahrensverzeichnisse sind ein Muss, sobald personenbezogene Daten regelmäßig verarbeitet werden

Verfahrensverzeichnisse sind ähnlich wie eine Inventur der Datenverarbeitung. Diese wird vor allem dann notwendig, wenn personenbezogene Daten regelmäßig verarbeitet werden. Und dann müssen Träger, Vereine oder Körperschaften diese Verfahrensverzeichnisse erstellen. Im **Artikel 30 DSGVO** ist festgehalten, was in diesem Verzeichnis stehen muss. **Alle verarbeiteten Daten müssen sowohl in technischer als auch organisatorischer Hinsicht geschützt werden, Artikel 32 DSGVO**.

Privacy by Design: Nur Daten verarbeiten, für die man eine Rechtsgrundlage hat und bestenfalls so wenige wie möglich

Artikel 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten: > Welche Rechtsgrundlage habe ich, um Daten zu erheben? > Daten-Minimierung: Welche Daten brauche ich wirklich? > Art. 37 DSGVO: Braucht man einen Datenschutzbeauftragten?

> Nichtöffentliche Stellen

Wenn mindestens 20 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden oder wenn man die Verarbeitung vornimmt, die einer sogenannten Datenschutz-Folgenabschätzung unterliegen.

> Öffentliche Stellen

Brauchen immer einen Datenschutzbeauftragten nach **§ 5 BDSG** (Körperschaften des öffentlichen Rechts)

Tipps (gilt für Ehren- und Hauptamt)

> Wenn Personen per E-Mail für die Organisation kommunizieren sollen, sollten sie auch eine E-Mail-Adresse erhalten. Dadurch kann man sicherstellen, dass Sie Zugriff auf diese E-Mails haben und datenschutzkonform damit umgehen können.

> Personen sollten in den Umgang mit Daten in die technisch-organisatorischen Maßnahmen eingeführt werden.

> Organisationsfremde und Externe dürfen keinen Zugriff auf die Daten haben .

Weitere Datenschutzpflichten

> Auftrags- und Trennungskontrolle

> Sicherstellung von Integrität und Vertraulichkeit sowie Wiederherstellbarkeit

> Pflicht zur Anonymisierung und Pseudonymisierung, wo es nötig oder möglich ist

> Eine Datenschutz-Folgenabschätzung muss erfolgen, wenn die Verarbeitung personenbezogener Daten ein hohes Risiko für die Betroffenen birgt.

neueste regelungen: netzdg und digital services act

Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz–NetzDG) ist seit dem 1. Oktober 2017 in Kraft.

Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken
Netzwerkdurchsetzungsgesetz – NetzDG

Das Gesetz zielt darauf, Hasskriminalität, strafbare Falschnachrichten und andere strafbare Inhalte auf den Plattformen sozialer Netzwerke wirksamer zu bekämpfen. Dazu zählen z. B. Beleidigung, üble Nachrede, Verleumdung, öffentliche Aufforderung zu Straftaten, Volksverhetzung, Gewaltdarstellung und Bedrohung. Um die sozialen Netzwerke zu einer zügigeren und umfassenderen Bearbeitung von Beschwerden insbesondere von Nutzerinnen und Nutzer über Hasskriminalität und andere strafbare Inhalte anzuhalten, wurden mit dem NetzDG gesetzliche Compliance-Regeln für soziale Netzwerke eingeführt. Dies beinhaltet eine gesetzliche Berichtspflicht für Anbieterinnen und Anbieter sozialer Netzwerke über den Umgang mit Hasskriminalität und anderen strafbaren Inhalten, Vorgaben zum Vorhalten eines wirksamen Beschwerdemanagements sowie zur Benennung eines inländischen Zustellungsbevollmächtigten. Verstöße gegen diese Pflichten können mit Bußgeldern gegen das Unternehmen und die Aufsichtspflichtigen geahndet werden. Außerdem wird Opfern von Persönlichkeitsrechtsverletzungen im Netz ermöglicht, aufgrund gerichtlicher Anordnung die Bestandsdaten der Verletzerinnen und Verletzern von den Diensteanbietenden zu erhalten. QR-Code 28

Das Gesetz für Digitale Dienste/ Digital Services Act *DSA*

Der DSA will ein freies und demokratisches Internet sichern. Das Gesetz erleichtert die Entfernung illegaler Inhalte und schützt die Grundrechte der Nutzer:innen – darunter die Redefreiheit – im Internet. Außerdem sorgt es für eine strengere Beaufsichtigung von Online-Plattformen, insbesondere von Plattformen, die mehr als 10 % der EU-Bevölkerung erreichen.

Weitere Informationen QR-Code 29
YouTube-Video QR-Code 30

Inhalte des DSA *(unter anderem)*

> **Wirksame Schutzvorkehrungen** für die Nutzer:innen mit der Möglichkeit, Entscheidungen der Plattformen zur Moderation von Inhalten anzufechten

> **Verbot bestimmter Arten gezielter Werbung** auf Online-Plattformen (wenn sie auf Kinder abzielen oder besondere personenbezogene Daten wie ethnische Zugehörigkeit, politische Ansichten, sexuelle Ausrichtung nutzen)

> **Erhöhung der Transparenz von Online-Plattformen** in unterschiedlichen Bereichen, unter anderem bei den verwendeten Algorithmen Zugriff für die Forschung auf die Kerndaten größerer Plattformen und Suchmaschinen, um das Fortschreiten von Online-Risiken nachvollziehen zu können

online-sicherheit in zeiten von online-hass

Josephine Ballon

Rechtsanwältin und
Head of Legal bei HateAid

Josephine Ballon ist Rechtsanwältin und Head of Legal bei HateAid. Dort berät sie von digitaler Gewalt betroffene Individuen, Organisationen sowie Zusammenschlüsse von Aktivist:innen und unterstützt sie bei der Rechtsdurchsetzung. Die Organisation HateAid ist eine Beratungsstelle für Betroffene von digitaler Gewalt.

Was sind die häufigsten Anwendungsfälle von digitaler Gewalt gegen Organisationen?

> Anfeindungen und Drohungen gegen die Organisationen als solche
Dies hat im Kontext der Corona-Pandemie zugenommen und ist häufig von aktuellen Ereignissen abhängig.

> Anfeindungen und Drohungen gegen die Mitarbeitenden
Vor allem in einem aktivistischen Kontext oder in der Arbeit mit Ehrenamtlichen lässt sich das Privat- und Berufsleben nicht immer trennen und verschwimmt sehr schnell im Internet, wenn es um Auftritte auf Social Media oder anderen Online-Plattformen geht.

> Verleumdungen
Wenn über Organisationen Lügen verbreitet werden, um sie zu diskreditieren oder ihre Legitimation zu untergraben, sich für ein bestimmtes Themenfeld zu engagieren, ist dies ein Fall von Verleumdung.

> Angriffe auf Accounts von Organisationen
Dazu zählen das Hacking und das Phishing, wobei Passwörter abgegriffen wurden, um auf die Accounts einzuwirken.

> DOXXING
Dabei werden sensible Daten gestohlen und öffentlich gemacht.

Josephine Ballon

Online-Hass ist kein Zufall, sondern Strategie

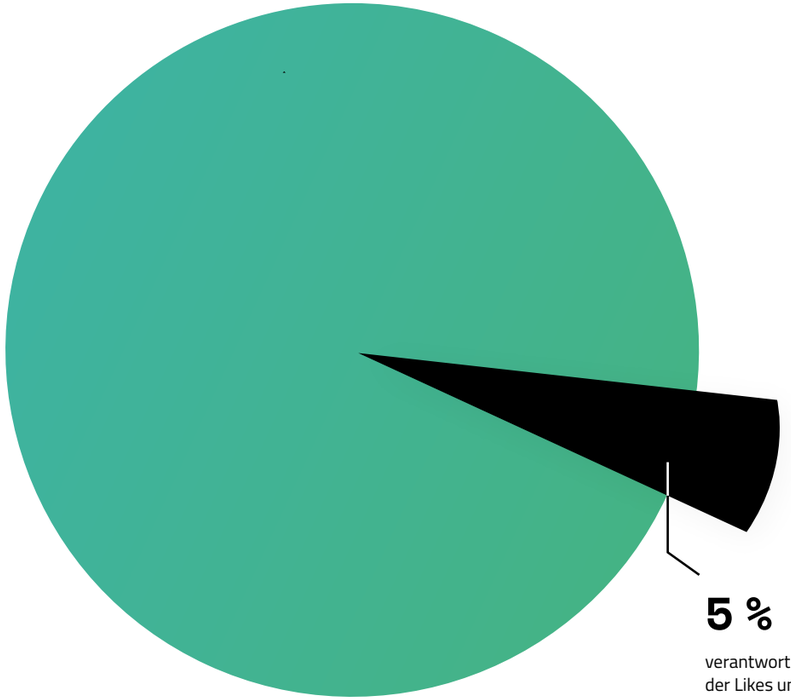
Hass und digitale Gewalt passieren nicht durch „verwirrten Einzelpersonen", die plötzlich hasserfüllt geworden sind und im Internet dazu veröffentlichen. Aus Erhebungen weiß man, dass es wenige sind, die den Hass verbreiten, damit jedoch einen gewaltigen Effekt verursachen. Diese Personen nutzen bewusst die Algorithmen sozialer Netzwerke sowie andere Gegebenheiten des Internets. Wir wissen aus einer Erhebung, die auf Facebook durchgeführt wurde:

Nur 5 % der User, die sich an Diskussionen beteiligt haben, die in den Kommentarspalten mit besonders hasserfüllter Sprache stattgefunden haben, waren daraufhin für 50 % der Likes unter den Hasskommentaren verantwortlich.

Aus Zahlen des Bundeskriminalamts ist bekannt, dass digitale Gewalt vor allem aus dem rechten und rechtsextremen Spektrum kommt. Die Strategie dahinter ist, Menschen einzuschüchtern und aus dem Diskurs zu verdrängen, sowie diesen zu verschieben.

Strategische Verzerrung von Online-Diskursen

Nur ein Bruchteil aller User:innen forciert überproportional Hass-Kommentare



5 %

verantwortlich für 50 % der Likes unter den Hasskommentaren

Der SILENCING Effekt ist eine der Folgen von Online Hass

Der Hass, der sich im Internet verbreitet, wirkt sich nicht nur auf diejenigen aus, die tatsächlich angegriffen werden, sondern auch auf die Mitlesenden. Es ist nachgewiesenes Ziel und leider auch das Ergebnis, dass 54 % der Internetnutzer:innen sich nicht mehr trauen, im Netz ihre politische Meinung zu sagen – der sogenannte Silencing Effekt.

Das heißt auch, die Mitlesenden sollen eingeschüchtert werden. Es geht darum, sie aus dem öffentlichen Diskurs zu verdrängen, um diesen in eine einseitige Richtung zu verschieben und gleichzeitig den Eindruck zu erwecken, dass diejenigen, die Hass und digitale Gewalt verbreiten, in der Mehrheit sind, obwohl das gar nicht zutreffend ist.

Organisationen stehen vor verschiedenen Herausforderungen

Es muss grundsätzlich damit gerechnet werden, dass die Täter:innen sehr internetaffin sind und verstehen, wie digitale Gewalt wirkt.

Direkte und indirekte Folgen von Online-Hass

Mitlesende sollen ebenso eingeschüchtert werden wie direkte Opfer von Angriffen

54 %

davon betroffen von Silencing Effekt

Konkrete Herausforderungen für Organisationen

- **IT-Infrastruktur und Geräte absichern**
- **„analoge" Sicherheit der Mitarbeiter:innen**
  - Räumlichkeiten
  - Datenschutz z. B. auch bei Öffentlichkeitsarbeit (v. a. Namen und Bilder)
- **Schutz von Klient:innendaten**
- **Rechtliches Vorgehen gegen Angriffe digitaler Gewalt**
  - Aufwand für Beweissicherung, Rechtsberatung, Kostenrisiken

Rechtliches Vorgehen gegen Angriffe digitaler Gewalt: Kosten und Risiken
HateAid bietet Prozesskosten-Finanzierung an. Das heißt Einzelpersonen und Unternehmen können rechtlich gegen Angriffe digitaler Gewalt, gegen die Täter und Täterinnen oder gegen die Plattformen ohne eigenes Kostenrisiko vorgehen. Organisationen schrecken oftmals davor zurück, gegen Angriffe vorzugehen, weil es mit viel Aufwand verbunden ist. Vor allem Fragen der Beweissicherung verursachen viel Mühe und Bedarf für Rechtsberatung. Wenn das eigene rechtliche Know-How nicht ausreichend ausgeprägt ist, muss man Externe dazuschalten. Kostenrisiken von rechtlichem Vorgehen gehen über die Anwaltskosten hinaus, sondern erstrecken sich zum Beispiel auch auf die Gerichtskosten.

Was können Organisationen tun, um sich und ihre Mitarbeitenden zu schützen?

Sichere IT-Infrastruktur und Geräte

Die Mitarbeitenden müssen entsprechend geschult und sensibilisiert werden. Dazu zählen die Verwendung sicherer Passwörter und eines Passwort Managers, um sicherzugehen, dass die Passwörter nicht leicht zu erraten sind. Zwei Faktor Authentifzierung, die auf allen Geräten und bei allen Konten, wo es möglich ist, zu verwenden ist und natürlich keine Nutzung privater Endgeräte und keine Überschneidungen zwischen dienstlich genutzten und privaten Geräten, da Angriffe auf Privatgeräte sonst die Organisation gefährden. Gleichzeitig wird ein Phishing Training empfohlen, um aufzuzeigen, welche Möglichkeiten es für Externe gibt, sich Zugang zu bestimmten Konten zu erschleichen.

Schutz von externen Daten: sparsamer Umgang und Pseudonymisierung

Im Fokus stehen vor allem Klient:innen-Daten sowie andere sensible Daten, die gemeinnützige Organisationen schützen müssen. Im gemeinnützigen Sektor ist es zentral, die Klient:innen zu schützen, die Glaubwürdigkeit nach außen sowie die Vertrauenswürdigkeit gegenüber den öffentlichen Geldgebern zu erhalten. Das heißt, **externe Daten sind sparsam zu behandeln und wo es geht zu pseudonymisieren.**

Analoge Maßnahmen

Dies betrifft bereits die Auffindbarkeit der Räumlichkeiten und ihre Sicherung. > Wie werden die Namen und Informationen über Mitarbeitende gesichert? > Wie wird die Öffentlichkeitsarbeit gestaltet? > Muss Bildmaterial verwendet werden? > Ist es erforderlich, mit vollem Namen aufzutreten? All dies muss eine Organisation abwägen und in engen Austausch mit den Mitarbeitenden treten, damit sie sich nicht angreifbar machen.

Privatsphäre-Check

Nachdrücklich anzuraten ist ein Privatsphäre-Check. Mitarbeitende sollten dazu angehalten werden, sich selbst zu googeln und dabei bis zu Seite fünf der Google-Suchergebnisse zu schauen sowie andere Suchmaschinen auszuprobieren und die Profil Einstellungen der sozialen Netzwerke zu überprüfen. Denn nicht alles, was man im privaten Kontext über sich preisgibt, soll für alle einsehbar sein, die in einem anderen Kontext über Suchmaschinen den Namen zu finden versuchen. Bei Bedarf sollten Mitarbeitende hierbei unterstützt werden.

In Betracht zu ziehen ist zusätzlich eine Melderegistersperre nach § 51, **Bundesmeldegesetz**.

Melderegistersperre, § 51 Bundesmeldegesetz *BMG*

> Voraussetzung: Melderegisterauskunft stellt potentiell Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen dar

> Schutz vor Bedrohung, Beleidigung und unbefugter Nachstellung, auch wegen beruflicher oder ehrenamtlicher Tätigkeit

> Ggf. **Empfehlungsschreiben von Beratungsstelle o. Ä. einholen**

> Ziel : Privatpersonen, Unternehmen, Rechtsanwälte erhalten keine Informationen

> Warum? Selbst Privatpersonen können ohne besondere Begründung bei der Meldebehörde Einsicht verlangen, Angabe des „berechtigten Interesses" wird nicht überprüft (Eine Behauptung, dass eine bestimmte Person zum Beispiel Geld schuldet und man sie verklagen möchte, reicht aus, um die Adresse der Person von der Melderegisterauskunft zu erhalten.)

> Wo? Meldebehörde des Wohnsitzes QR-Code 31

> Wie? Formloser Antrag

> Was ist mitzuführen? Ausweisdokument, Dokumente zur Glaubhaftmachung (Urteile, Bestätigung der Polizei, Strafanzeigen, Stellungnahmen einer Beratungsstelle)

In Deutschland ist es sehr einfach, an die Privatanschrift von Menschen zu gelangen, wenn man ihren Namen, ihr Geburtsdatum oder eine frühere Adresse kennt. Um das Geburtsdatum zu erfahren, kann es ausreichen, Geburtstagsgrüße auf der Facebook-Timeline zu finden. Alte Adressen finden sich häufig in Einträgen von Telefonbuchanbietern, zum Beispiel bei „Das Örtliche". Die Daten der Privatanschrift sind besonders schützenswert, da bei Auffindbarkeit im Netz eine konkrete Gefahr für die Personen entstehen kann.

Die Impressumspflicht

Das Gesetz schreibt vor, dass ein Impressum für geschäftsmäßige Diensteanbieter notwendig ist, dies umfasst auch die Webseite einer gemeinnützigen Organisation. Man ist verpflichtet, den **Namen** und die **Anschrift** einer Niederlassung sowie die **Registernummer** anzugeben. Bei Menschen, die sich aktivistisch einsetzen, ist dies leider häufig die Privatadresse, da sie keine geschäftlichen Räumlichkeiten anbieten. Bei Organisationen ist dies die registrierte Anschrift, auch wenn sie grundsätzlich schwieriger auffindbar gemacht werden sollte.

Trick:
Das Impressum nicht als Textdatei auf der Webseite hinterlegen, sondern als Bild / Screenshot. So ist die Adresse über Suchmaschinen nicht auffindbar und man kann nicht gezielt nach der Adresse suchen, auch wenn sie trotzdem jederzeit auf der Seite steht.

Was versteht man unter „Anschrift”?
Mindestens der Name muss im Impressum genannt werden, wenn es um eine Privatperson geht, mit Vor- und Nachnamen, bei Organisationen muss die vollständige Organisationsbezeichnung mit der jeweiligen Rechtsform angegeben werden. Bei der Anschrift selbst sind die Vorgaben ungenau. Es wird in der Regel verlangt, dass eine ladungsfähige Anschrift angegeben wird. Das bedeutet: Es muss eine gewisse Gewähr dafür gegeben sein, dass es eine ernsthafte Möglichkeit der Zustellung von Dokumenten gibt und dass man dort mit gewisser Wahrscheinlichkeit angetroffen werden kann. Letztendlich muss sichergestellt sein, dass Behördenbriefe empfangen werden können und dies nicht mit einer Verzögerung geschieht, die die Einhaltung von Fristen gefährdet. **Im Fall der Anschrift muss man abwägen, was gewichtiger ist: die Gefahr, dass man eine Abmahnung erhält, wenn man die Anschrift nicht angibt oder die mögliche Gefährdung bei Offenlegung.** Es gibt keine rein juristisch gute Antwort darauf. Ob die Anschrift eines Rechtsanwaltes genutzt werden kann, ist sehr umstritten. Es gibt Rechtsanwälte, die anbieten, ihre Kanzlei-Anschrift und ihre Vertretung als Impressumsanschrift anzugeben. Ob dies gesetzeskonform ist, wurde durch Gerichte bisweilen nicht erprobt. Wenn man als Organisation darüber nachdenkt, eine Anschrift anzugeben, an der man de facto nicht registriert ist, muss man natürlich bedenken, dass eine Registerabfrage trotzdem möglich ist. Dies unterliegt jedoch einer höheren Hemmschwelle, als auf der Webseite zu schauen.

Wie können sich Organisationen gegen digitale Gewalt wehren?
Auf eigenen Kanälen und Social Media Seiten darf man Kommentare oder Nachrichten löschen und verbergen. Wenn man auf öffentlichen Social Media Seiten angefeindet wird, kann man diese Inhalte immer nach dem **Netzwerkdurchsetzungsgesetz** (Stand: Juni 2021) melden. Dann sind die Plattformen verpflichtet, diese Inhalte zu löschen, weil sie bestimmte Straftatbestände erfüllen. Bei Google Suchmaschinen-Einträgen, die auf unliebsame Webseiten verweisen, kann man über einen Löschantrag erwirken, dass diese Seiten nicht mehr gefunden werden können.

Beweissicherung ist beim rechtlichen Vorgehen gegen digitale Gewalt essentiell
Bevor man darüber nachdenkt, etwas zu löschen, muss man sich immer mit dem Thema der Beweissicherung beschäftigen. Es reicht nicht, ein Foto vom Bildschirm zu machen, sondern Datum und Uhrzeit des jeweiligen Inhalts müssen erkennbar sein sowie der jeweilige User-Name oder, wenn möglich, Klarname der potenziellen Täter:innen. Auch der Kontext muss ersichtlich sein, da sich die juristische Bewertung von Beleidigungen und ähnlichem häufig aus dem Kontext ergibt. Zusätzlich sollte die URL zu den Inhalten, wenn sie noch verfügbar sind, angegeben werden. Man kann dafür frei verfügbare Online Tools verwenden, die mit Zeit- und Datumsstempel arbeiten. Grundsätzlich kommt es darauf an, glaubhaft zu machen, dass alles tatsächlich so passiert ist. Vor allem bei Beleidigungen, Drohungen, Verleumdungen gegen die Mitarbeitenden, aber auch gegen die Organisation als solches, ist eine Strafanzeige in Betracht zu ziehen.

Wie können sich Organisationen wehren, wenn sie beleidigt werden?
Organisationen, die im Prinzip einen abgegrenzten Personenkreis ausmachen, können als bestimmbare Adressaten beleidigt und verleumdet werden. Von Beleidigungen in Abgrenzung von einer Meinungsäußerung spricht man, wenn das Gegenüber ohne jeglichen Sachbezug herabgewürdigt wird sowie wenn Schimpfwörter und Fäkalsprache benutzt werden. **Auch auf Social Media sind Beleidigungen strafbar**. Natürlich muss man insbesondere, wenn man sich zu einem umstrittenen Thema positioniert, Kritik hinnehmen. Doch wenn das erkennbare Ziel ist, eine Person oder Organisation öffentlich bloßzustellen, handelt es sich um einen Beleidigungstatbestand.

Was erfüllt den Tatbestand der üblen Nachrede und Verleumdung?
Es gilt nicht als Beleidigung, wenn es um unwahre Tatsachenbehauptungen geht, die in irgendeiner Form jedoch einem Beweis zugänglich sind. Die Inhalte müssen geeignet sein, herabzuwürdigen oder verächtlich zu machen. Weiß der Verfasser oder die Verfasserin, dass eine Behauptung nicht wahr ist, spricht man von Verleumdung. Kann er oder sie die Wahrheit nicht beweisen, gilt es als üble Nachrede. Man sollte immer darauf achten, was man im Netz teilt und Quellen hinterfragen, die man weiterverbreitet. Denn, wenn es öffentlich passiert, kann es auch sehr schnell strafbar sein.

Zu Volksverhetzung zählt im Antisemitismus-Kontext auch Holocaust-Leugnung und Holocaust-Verharmlosung
Volksverhetzung ist im Antisemitismus-Kontext sehr relevant. Man spricht von Volksverhetzung, wenn Bevölkerungsgruppen oder Einzelpersonen, weil sie zu einer Bevölkerungsgruppe gehören, angefeindet werden, wenn gegen sie zum Hass aufgestachelt wird, zu Gewalt gegen sie aufgerufen wird, beschimpft oder verleumdet wird und / oder wenn das in einer Art und Weise passiert, die diese Gruppe als möglicherweise gefährlicher für die Öffentlichkeit erscheinen lässt. **Beim Tatbestand der Volksverhetzung gibt es in Deutschland den Sonderfall, dass Holocaust-Leugnung und Holocaust-Verharmlosung ebenfalls Straftaten sind.** Volksverhetzung sollte unbedingt angezeigt werden.

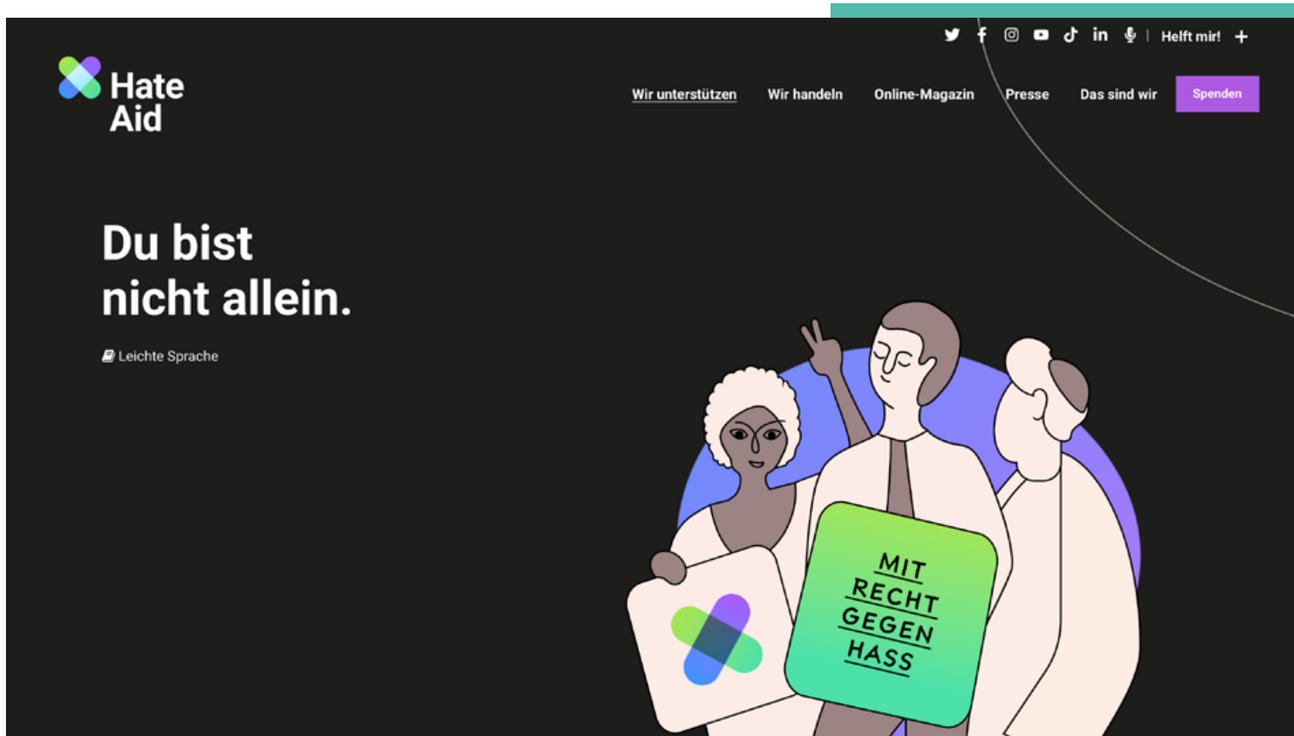
Das Teilen von verfassungsfeindlichen Symbolen ist eine Straftat
Es ist eine Straftat, verfassungsfeindliche Symbole zu zeigen, selbst, wenn dies „nur aus Spaß" auf Social Media geschieht. Hier gilt dasselbe wie für Volksverhetzung: Es lohnt sich, Strafanzeige zu stellen, denn diesen Tatbestand nehmen Ermittlungsbehörden sehr ernst.

Strafanzeige zu stellen, hilft nicht nur den Betroffenen, sondern zeigt auch strukturelle Probleme auf
Beleidigungen werden leider zu wenig angezeigt, denn Betroffene und auch Organisationen können nicht immer eine korrekte Einordnung der Rechtslage durchführen. Wenn man den Eindruck hat, dass etwas die Schwelle zur Strafbarkeit überschritten haben könnte, sollte man es zur Anzeige bringen.
Nur wenn Anzeigen erstattet werden und bei den Ermittlungsbehörden eingehen, erkennen sie ein strukturelles Problem. Nur so wird deutlich, dass nicht nur Einzelfälle betroffen sind, sondern dass Handlungsbedarf besteht und die Behörden zum Beispiel durch Schaffung von Sonderabteilungen für Hass im Netz aktiv werden müssen. Von Strafanzeigen können wir uns deshalb nachhaltige Effekte erhoffen. Man kann Strafanzeigen bei jeder Polizeidienststelle, bei der Staatsanwaltschaft oder über HateAid durch eine E-Mail oder den Einsatz der App „Meldehelden" erstatten. Falls Beweise nicht perfekt gesichert sind, bereitet HateAid sie auf und leitet alles an eine spezialisierte Staatsanwaltschaft weiter. Grundsätzlich kann man auch mündlich Strafanzeige stellen. Ausnahmen gelten bei Beleidigungen und ähnlichem. Hierbei muss man schriftlich einen Strafantrag stellen, der handschriftlich unterschrieben sein muss und besagt: „Ich möchte, dass das verfolgt wird, da es eine Beleidigung gegen mich ist."

Zivilrechtliche Möglichkeiten gegen Hass im Netz vorzugehen
Die Verfolgung einer Strafanzeige wird leider häufig eingestellt. Es gibt jedoch auch zivilrechtliche Möglichkeiten, um gegen Hass im Netz vorzugehen, wenn man verleumdet, beleidigt oder bedroht wird. Im Gegensatz zum Strafverfahren, wo es darum geht, dass der Staat den Täter oder die Täterin durch eine Geld- oder Freiheitsstrafe bestraft, kann man konkret von einer Person, die einen bestimmten Kommentar verfasst hat, eine Nachricht oder eine E-Mail geschickt hat, verlangen, dass der Inhalt auf allen Plattformen gelöscht wird, auf denen er verbreitet worden ist. Es wird gefordert, dass die Verbreitung der Inhalte sich nicht wiederholt, dass die Kosten getragen werden und in besonders extremen Fällen von Persönlichkeitsrechtsverletzungen eine Entschädigung als Schmerzensgeld gezahlt wird. Außergerichtlich passiert dies durch einen Rechtsanwalt oder eine Rechtsanwältin, der oder die eine Abmahnung schickt. Falls das nicht funktioniert oder wenn es schnell gehen muss, kann man über eine einstweilige Verfügung oder eine Klage nachdenken. Dabei können die Kosten von HateAid übernommen werden. HateAid berät Organisationen, leitet Workshops und setzt sich dafür ein, dass es Betroffene in Zukunft leichter haben, rechtlich gegen Online-Hass vorzugehen.

Aktuelle Informationen zur Arbeit von HateAID
QR-Code 32

Wer von digitaler Gewalt betroffen ist, findet bei HateAID Unterstützung (Fälle können hier gemeldet werden)
QR-Code 33



10 grundsätze für digitale sicherheit

01

Sichere IT-Infrastruktur und Geräte: Regelmäßige Sicherheitsupdates durchführen und immer die aktuelle Software verwenden

02

Sicheres Passwortmanagement, 2-Faktor-Authentifizierung und Privatsphäre-Einstellungen überprüfen

03

Phishing-Mails und betrügerische Websites erkennen lernen

04

Niemals private E-Mail-Adressen für Arbeitszwecke nutzen

05

Präventive Maßnahmen, Informations-, IT- und Cybersicherheit für die Organisation definieren

06

Regelmäßige Backups aller wichtigen Daten

07

Sparsamer Umgang mit Daten und Einwilligungen: Nur das abfragen, was unbedingt nötig ist

08

Daten nicht lokal, sondern zentral, z. B. in einer datenschutzkonformen Cloud, speichern

09

Beweissicherung bei Online-Hass und Gewalt vornehmen und rechtlich vorgehen

10

Den Ernstfall eines Cyber-Angriffs genau planen und Verantwortlichkeiten festlegen

qr-code-verzeichnis

Öffnen Sie die Handy-Kamera und richten Sie sie auf den QR-Code, um somit auf die entsprechende Internetseite zu gelangen und sich zum jeweiligen Thema zu informieren.

1
Blog IT-Security (S. 4)

2
APT (S. 5)

3
Backup (S. 5)

4
Cloud (S. 5)

5
CMS (S. 6)

6
Credentials (S. 6)

7
Cyberkriminalität (S. 6)

8
Darknet (S. 6)

9
Deep Fakes (S. 7)

10
DOS (S. 7)

11
Doxxing (S. 7)

12
exe-Datei (S. 7)

13
Hacker (S. 8)

14
Host Provider (S. 8)

15
IP-Adresse (S. 8)

16
Malware (S. 8)

17
Patch (S. 9)

18
Phishing (S. 9)

19
Ransomware (S. 9)

20
Script (S. 9)

21
Silencing (S. 10)

22
(Web-)Tracking (S. 10)

23
Webanalyse Tools (S. 10)

24
Wordpress (S. 10)

25
DSGVO (S. 18)

26
DSGVO (S. 18)

27
DSGVO (S. 22)

28
NetzDG (S. 27)

29
Gesetz dig. Dienste (S. 27)

30
YouTube Video (S. 27)

31
Meldebehörde (S. 35)

32
HateAID Infos (S. 40)

33
HateAID Hilfe (S. 40)

quellen

1 Blog IT-Security (S. 4)
https://www.is-its.org/it-security-blog

2 APT (S. 5)
https://www.computerweekly.com/de/definition/Advanced-Persistent-Threat-APT#:~:text=APT%2DGruppen%20verschaffen%20sich%20Zugang,Sich%20im%20Ziel%20etablieren

3 Backup (S. 5)
https://www.ionos.de/digitalguide/server/sicherheit/was-ist-ein-backup/

4 Cloud (S. 5)
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cloud-Computing-Sicherheitstipps/Grundlagenwissen/grundlagenwissen_node.html;jsessionid=801115402561A4F1D0E98FCE3BB3DE71.internet482

5 CMS (S. 6)
https://www.textbroker.de/content-management-system

6 Credentials (S. 6)
https://www.itwissen.info/Credential-credential.html

7 Cyberkriminalität (S. 6)
https://www.avast.com/de-de/c-cybercrime

8 Darknet (S. 6)
https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet

9 Deep Fakes (S. 7)
https://www.bundesregierung.de/breg-de/themen/umgang-mit-desinformation/deep-fakes-1876736#:~:text=Deep%20Fakes%20sind%20t%C3%A4uschend%20echt,Hilfe%20von%20k%C3%BCnstlicher%20Intelligenz%20erzeugt.

10 DOS (S. 7)
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html#:~:text=Denial%20of%20Service%20%E2%80%93%20oder%20kurz,und%20im%20schlimmsten%20Fall%20zusammenbricht.

11 Doxxing (S. 7)
https://www.avast.com/de-de/c-what-is-doxxing#topic-1

12 exe-Datei (S. 7)
https://www.it-business.de/was-ist-eine-exe-datei-a-751483/

13 Hacker (S. 8)
https://www.security-insider.de/was-ist-ein-hacker-a-596399/

14 Host Provider (S. 8)
https://www.rankeffect.de/mag/online-marketing/hoster-hosting-provider/

15 IP-Adresse (S. 8)
https://www.kaspersky.de/resource-center/definitions/what-is-an-ip-address

16 Malware (S. 8)
https://www.avast.com/de-de/c-malware

17 Patch (S. 9)
https://www.myrasecurity.com/de/patch/

18 Phishing (S. 9)
https://www.security-insider.de/was-ist-phishing-a-591842/

19 Ransomware (S. 9)
https://www.kaspersky.de/resource-center/threats/ransomware

20 Script (S. 9)
https://seiten-werk.com/lexikon/script/

21 Silencing (S. 10)
https://www.medienradar.de/hintergrundwissen/artikel/zwischen-beleidigungskultur-und-silencing

22 (Web-)Tracking (S. 10)
https://praxistipps.chip.de/was-ist-tracking-einfach-erklaert_41929

23 Webanalyse Tools (S. 10)
https://de.ryte.com/wiki/Webanalyse_Tools#:~:text=Webanalyse%2DTools%20dienen%20der%20%C3%9Cberpr%C3%BCfung,gesammelt%20werden%2C%20grafisch%20sichtbar%20machen.

24 Wordpress (S. 10)
https://www.seo-analyse.com/seo-lexikon/w/wordpress/

25 DSGVO (S. 18)
https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_de

26 DSGVO (S. 18)
https://eu-datenschutz-grundverordnung.net/eu-dsgvo/

27 DSGVO (S. 22)
https://eu-datenschutz-grundverordnung.net/eu-dsgvo/

28 NetzDG (S. 27)
https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html

29 Gesetz dig. Dienste (S. 27)
https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_de

30 YouTube Video (S. 27)
https://www.youtube.com/watch?v=BjxsulTe4pg

31 Meldebehörde (S. 35)
https://www.melderegister-auskunft.de/

32 HateAID Infos (S. 40)
https://hateaid.org/

33 HateAID Hilfe (S. 40)
https://hateaid.org/betroffenenberatung/