

# Digitale Sicherheit & Verantwortung

Aktuell diskutierte Gesetze wie die geplante Novelle des Telekommunikationsgesetzes, das **IT-Sicherheitsgesetz 2.0** und das sogenannte **BND-Gesetz** verleihen Sicherheitsbehörden das Recht, IT-Systeme zu hacken. Dafür werden Schwachstellen gebraucht, die es gar nicht geben dürfte und die vom Staat eliminiert werden müssten. Wie sieht das Bedrohungspotenzial durch **Cyberkriminalität** für die deutsche Wirtschaft aus? Aufschluss gibt die eco Umfrage zur IT-Sicherheit 2021. Für das Gute und mehr **Verantwortung im Netz** setzt sich die eco **Beschwerdestelle** ein. Im Kampf gegen Kinderpornografie, Volksverhetzung sowie Gewalt im Netz kann sich Jede und Jeder engagieren.

## AKTUELLE GESETZESVERFAHREN

In den Plänen zu aktuellen Gesetzesvorhaben sieht der eco Verband einen Trend zum staatlichen Hacking: **99,9 Prozent** aller weltweiten Datenverkehre dürften vom Bundesnachrichtendienst überwacht werden, sollte das geplante BND-Gesetz in dieser Form umgesetzt werden. Dazu soll das BSI mittels des IT-Sicherheitsgesetzes 2.0 weitere Befugnisse erhalten, um IT-Unternehmen umfassend zu kontrollieren, der Öffentlichkeit aber gleichzeitig wichtige Sicherheitsinformationen vorenthalten dürfen. ecos stellvertretender Vorstandsvorsitzender Klaus Landefeld spricht im **Podcast „Das Ohr am Netz“** und im **Deutschlandfunk** über weitreichende Folgen sowie den Vertrauensverlust der Bevölkerung in digitale Kommunikation und Anwendungen, den die Politik durch die Gesetze bezwecken würde.

## GEMEINSAM FÜR DAS GUTE IM NETZ

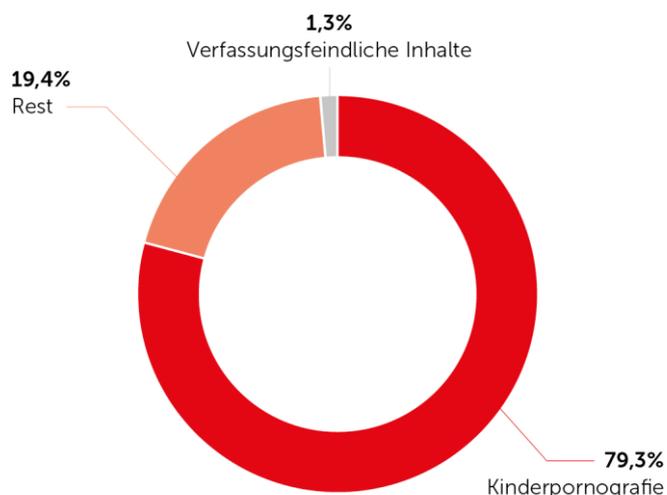
Seit **25 Jahren** bekämpft die **eco Beschwerdestelle** erfolgreich illegale Inhalte im Netz: Im Jahr 2020 konnten **97,7 Prozent** der monierten Inhalte entfernt oder anderweitig legalisiert werden, zum Beispiel mit einer Altersbeschränkung für Kinder und Jugendliche. Weniger als ein Fünftel der beanstandeten URLs war dabei in Deutschland gehostet. Gleichzeitig war die Zahl berechtigter Beschwerden mit klarem Rechtsverstoß mit insgesamt **5.523 Fällen im Jahr 2020** so hoch wie nie zuvor. Mehr als ein Drittel der Hinweise lieferten Bürger:innen (**21%** namentlich, **17%** anonym). Neben einem breiten Bündnis aus nationalen wie internationalen Netzwerkpartnern tragen Politik, Wirtschaft und Gesellschaft einen erheblichen Teil dazu bei, dass rechtswidrige Internet-



**77 Prozent** der deutschen **IT-Sicherheitsexpert:innen** gehen davon aus, dass die Bedrohungslage durch Cyberkriminalität für Unternehmen weiter steigen wird. Das geht aus der IT-Sicherheitsumfrage 2021 des eco Verbands hervor. Im Vorjahr waren noch **91 Prozent** von einer mindestens wachsenden Bedrohungslage ausgegangen. Weiter sieht mehr als die Hälfte der Befragten die deutsche Wirtschaft als unzureichend gegen Cyberangriffe aufgestellt (**57 %**). Besonders bedroht sind nach Einschätzung der Expert:innen kleine und mittelständische Unternehmen.

inhalte gelöscht und strafrechtlich verfolgt werden.

### Berechtigte Beschwerden 2020 (ohne Spam)



# Internetpolitische Forderungen

- Die Politik sollte im Dialog mit Anwendern und Anbietern einen gemeinsamen Ansatz für die Gestaltung von IT-Sicherheit verfolgen.
  - Der Einsatz und die Verwendung von Verschlüsselungstechnologien muss ausgebaut und gefördert werden.
  - Ermittlungen und Strafverfolgung im Netz dürfen nicht auf Kosten von Bürgerrechten sowie der Sicherheit von Diensten und Netzen gehen.
  - Der Staat darf die Verantwortung für die Rechtsdurchsetzung im Netz nicht auf private Unternehmen abwälzen.
  - Das **Notice and Take Down Prinzip** muss Basis und Grundlage für die europäische Rechtsdurchsetzung im Netz bleiben und darf nicht durch Uploadfilter oder andere nationale Gesetzgebung konterkariert werden.
- **Zur gesamten Internetpolitischen Agenda**

## STUDIEN UND LINKS

- [Kritik am IT-Sicherheitsgesetz 2.0](#)
- [IT-Sicherheitsumfrage 2021](#)
- [Jahresbericht der eco Beschwerdestelle 2020](#)