BUNDESARBEITSKAMMER

PRINZ-EUGEN-STRASSE 20-22
1040 WIEN
www.arbeiterkammer.at
erreichbar mit der Linie D

RTR
Rundfunk und Telekom Regulierungs-GmbH
Mariahilfer Straße 77-79
1060 Wien

Per Mail an:
konsultationen@rtr.at

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65**	Fax **501 65**	Datum
	BAK/KS-GSt/DZ/BE	Mag Daniela Zimmer	DW 12722	DW 12693	20.10.2023

Stellungnahme zum Entwurf der 9. Novelle der Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 (KEM-V 2009)

Die Bundesarbeitskammer (BAK) bedankt sich für die Übermittlung des im Betreff genannten Entwurfes und nimmt dazu wie folgt Stellung:

Anruf-Spoofing ("Call ID Spoofing") liegt vor, wenn der Anrufer absichtlich eine falsche Anrufer-ID verwendet, um den Angerufenen über seine Identität zu täuschen und im Zuge des nachfolgenden Gesprächs zu überrumpeln. Betrüger nutzen diese Methode oft, um unter Vortäuschung, der Inhaber der Rufnummer zu sein, Personen zu übervorteilen, sie etwa dazu zu bringen, Geld zu übermitteln oder persönliche Daten preiszugeben. Gefälschte Vorwahlen erwecken dabei den Anschein, dass der Anruf vom Land des Angerufenen ausgeht. Dies erhöht die Wahrscheinlichkeit, dass der Anrufempfänger auch tatsächlich abhebt.

Ziel der in der KEM-V neu eingefügten Bestimmung ist es, bei derartigen missbräuchlichen Anrufen mit verfälscht angezeigter Rufnummer

- zumindest die tatsächliche Anzeige der Rufnummer zu unterbinden und
- (soweit möglich) den Anruf nicht zuzustellen.

BAK-Bewertung:

Die vorgeschlagenen Änderungen der KEM-V werden BAK-seits begrüßt. Nicht nur die RTR-Meldestelle „Rufnummernmissbrauch" verzeichnete in den vergangenen Monaten einen signifikanten Anstieg an einschlägigen Beschwerden von Konsument:innen. Auch die AK-Beratungseinrichtungen sind diesbezüglich mit einem wachsenden Beschwerdeaufkommen konfrontiert.

Die Gewährung einer nicht all zu langen Umsetzungsfrist ist überaus zweckmäßig, um potenzielle Opfer vor dieser Form von Rufnummernmissbrauch rasch zu schützen.

Erweiterung des Anwendungsbereichs: Die vorgesehene Bestimmung widmet sich ausschließlich dem Spoofing mit österreichischen Rufnummern innerhalb Österreichs. Vergleichbare Methoden mit österreichischen Rufnummern im Ausland, bei SMS oder mit ausländischen Rufnummern in Österreich sind von der Maßnahme nicht erfasst. Die RTR führt dabei in ihren Erläuterungen an, dass der Handlungsdruck in dem Maße wächst, wie andere Länder Abhilfemaßnahmen ergreifen. Es sei erwartbar, dass die Täter sich in der Folge auf Staaten konzentrieren, in denen noch keine Gegenmaßnahmen getroffen wurden. Diese Ausweichbewegungen könnten sich aber gleichermaßen in jenen Bereichen abzeichnen, die nicht in den Anwendungsbereich der Verordnung fallen. Die BAK hofft deshalb, dass im Dialog mit den Telekomanbietern und mit Blick auf die technische Entwicklung mittelfristig auch Schutzmaßnahmen zugunsten der nicht erfassten Bereiche ergriffen werden.

Die AK Tirol hat Anfragen von Konsument:innen zu Spoofing über einen längeren Zeitraum systematisch beobachtet. Sie geht davon aus, dass Betrugsversuche mit ausländischen Rufnummern weitaus häufiger (im Vergleich zum Missbrauch inländischer Rufnummern) in Österreich vorkommen, nicht zuletzt, um die Strafverfolgung zu erschweren. Entsprechend groß wäre auch hier der Schutzbedarf der Konsument:innen. Leider adressiert die vorliegende Novelle diesen Bereich nicht. Konsument:innen könnten sich in der falschen Sicherheit wiegen, allgemein vor Spoofing geschützt zu sein. Soweit sich bei europäischen (oder internationalen) Verbindungen keine ausreichend treffsicheren Abhilfemaßnahmen anbieten, regen wir zumindest an, auf EU-Ebene im Rahmen von BEREC nach Lösungen zu suchen. Vermutlich gibt es auch bei grenzüberschreitenden Missbrauchsversuchen zumindest nützliche Indizien, die vollautomatisch ausgewertet werden könnten. Zweifelhafte Verbindungen könnten zumindest mit der Warnung „Achtung vor einem möglichen Rufnummernmissbrauch!“ versehen werden.

Maßnahmen werden begrüßt: Die beiden Verpflichtungen erscheinen uns zum Schutz der Konsument:innen geeignet. Das Verbot der Rufnummeranzeige nach § 5a Abs 1a signalisiert dem Anrufempfänger, dass es sich jedenfalls um keine ihm bekannte Rufnummer handelt und hat insoweit Warnfunktion. Inwieweit Telekomanbieter auch treffsicher die Zustellung betrügerischer Anrufe unterbinden, sollte die RTR monitoren. Sie könnte dazu Berichtspflichten der Anbieter einführen, um auf diese Weise einen Überblick über die Zahl geblockter Anrufe und den Einsatz zeitgemäßer Validierungstechniken zu haben.

Rechtsfolgen definieren: Zweckmäßig wäre allerdings, klarzustellen, welche Rechtsfolgen entstehen, wenn Anbieter dieses Verbot ignorieren bzw eine Anrufvalidierung nicht am Stand der Technik vornehmen und auf Verbraucherseite dadurch ein Schaden eintritt. Adressat des Verbots ist offenbar (nur) jener Anbieter, der die Verbindung i.d.R. aus dem Ausland entgegennimmt. Dieser ist nicht zwangsläufig auch der Vertragspartner der betroffenen Konsumenten:innen.

Fantasienummern: Die BAK regt an, klarzustellen, dass sich die VO nicht nur auf Fälle bezieht, in denen vorhandene Rufnummern des österreichischen Rufnummernplans, sondern (soweit technisch denkbar) auch reine Fantasienummern missbräuchlich genutzt werden.

Infopflicht: Aus Transparenzgründen ist überdies anzudenken, die Betreiber dazu zu verpflichten, Konsument:innen mitzuteilen, dass ihre Rufnummern missbräuchlich verwendet wurden (um überhaupt eine Chance zu haben, fehlerhaft unterbundene Anrufe zu identifizieren oder unzutreffende Vorhaltungen, betrügerische Anrufe würden vom tatsächlichen Rufnummerninhaber stammen, aufklären zu können).

In diesem Zusammenhang wird an die Forderungen erinnert, die die AK Tirol bereits vor einigen Jahren an das zuständige Ressort BMVIT herangetragen hat. Vorgeschlagen wurde damals, dass der den Anruf vermittelnde Provider verpflichtet werden sollte, gegebenenfalls eine ergänzende schriftliche Information mitzusenden, aus welcher für den/die Nutzer:in hervorgeht, dass die angezeigte Rufnummer nicht mit der tatsächlichen technischen Zuordnung übereinstimmt. Nutzer:innen wären gewarnt und hätten es selbst in der Hand, die Gespräche anzunehmen oder während dieser entsprechend wachsam zu sein.

Zu bedenken ist, dass die vollständige Unterbindung der Zustellung eines Anrufes nach Prüfung der Authentizität doch einen erheblichen Grundrechtseingriff darstellt. Es besteht zwar zweifellos ein beträchtliches öffentliches Interesse daran, Konsument:innen vor betrügerischen Anrufen auf einfache und verlässliche Weise zu schützen. Bei Abwägung aller Für und Wider erscheint allerdings problematisch, dass Angerufene bei einer solchen Unterbindung gar nicht von dem versuchten Anruf erfahren. Da die Prüfung der Rufnummernauthentizität durch den ausführenden Provider im Entwurf nur kursorisch erklärt und die Wahl der Mittel allein den Betreibern überlassen wird, sind Fehler beim Herausfiltern betrügerischer Anrufe jedenfalls nicht ausgeschlossen.

Im Ergebnis entscheidet jedenfalls stets der Provider, ob Nutzer:innen ein Anruf durchgestellt wird oder nicht. Vor diesem Hintergrund wird angeregt, noch andere (gelindere) Optionen zu prüfen. Dazu zählt die von der AK Tirol seinerzeit vorgeschlagene Kennzeichnung mutmaßlich betrügerischer Anrufe (woraus sich eine Wahlmöglichkeit für die Angerufenen ergibt, diese anzunehmen oder nicht). Zumindest könnte aber eine nachträgliche Information betroffener Kund:innen über eine vorgenommene Anrufunterbindung vorgesehen werden.

SMS: Von der Novelle nicht erfasst sind überdies “SMiShing”-Angriffe, dh Phishing per Textnachricht. Handynutzer:innen erhalten dabei eine SMS, die vorgeblich von Freunden oder Firmen (zB Postdienstleistern, die über angeblich abholbereite Pakete beachrichtigen) stammt und sie dazu auffordert, einen Link zu öffnen. Wer der Aufforderung folgt, infiziert sein Endgerät mit Malware, wird Opfer von Datendiebstahl uvm. Mit Blick auf die unter Umständen erforderliche Verarbeitung von dem Kommunikationsgeheimnis unterliegenden Inhaltsdaten sind geeignete Maßnahmen selbstverständlich sorgfältig abzuwägen.

EU-Initiative: Abschließend regen wir noch an, sich im Rahmen von BEREC für eine wirksame und EU-weit einheitliche Vorgangsweise gegen diese Form von Cyberkriminalität einzusetzen.

Die BAK ersucht um Berücksichtigung der in der Stellungnahme angeführten Anregungen.

Unterzeichner	Bundeskammer für Arbeiter und Angestellte
Datum/Zeit-UTC	31.10.2023 15:16
Prüfhinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.