

Repeater richtig einsetzen: Signalverlängerung clever meistern

Category: Online-Marketing

geschrieben von Tobias Hager | 16. August 2025



Repeater richtig einsetzen: Signalverlängerung clever meistern

Du willst mehr WLAN-Reichweite, ohne dein Netzwerk in eine lahme Funklotterie zu verwandeln? Dann vergiss Marketing-Versprechen und lerne, wie ein Repeater wirklich wirkt – physikalisch, protokolltechnisch und strategisch. Dieser

Guide zerlegt Mythen, erklärt SNR, RSSI, MCS und Backhaul wie ein Ingenieur – und zeigt, wie du mit Repeatern Reichweite gewinnst, ohne Durchsatz und Stabilität zu ruinieren.

- Was ein Repeater technisch macht und warum Signalverstärkung nicht gleich bessere Verbindung bedeutet
- Repeater vs. Mesh vs. Access Point: Architekturwahl für Reichweite ohne Bandbreiten-Halbierung
- Linkbudget, dBm, SNR, MCS und Kanalbreite: die Zahlen, die über Erfolg oder Frust entscheiden
- Optimale Platzierung: RSSI-Fenster, EIRP-Grenzen, DFS-Kanäle und Störquellen im Griff behalten
- Installation Schritt für Schritt: dedizierter Backhaul, WPA3, Roaming-Optimierung und VLAN-Gastnetz
- Performance-Messung mit iPerf3, Spektrumanalyse, Airtime-Checks und realistischen Durchsatz-Tests
- Repeater im Mobilfunk- und IoT-Umfeld: 5G, LoRa, Outdoor und rechtliche Stolperfallen
- Sicherheit und Compliance: ETSI, CE, BNetzA, DFS, WPS-Fallen und Firmware-Strategien
- Fehlersuche wie ein Profi: Hidden Nodes, Interferenzen, Doppel-NAT, Latenzspitzen und Bufferbloat
- Klares Fazit: Repeater richtig einsetzen oder konsequent verkabeln – halbe Lösungen kosten Leistung

Ein Repeater klingt nach Magie: hinstellen, Knopf drücken, Reichweite verdoppeln. In der Praxis ist ein Repeater nur so gut wie das Eingangssignal, das Protokoll-Overhead und die Funkumgebung. Ein Repeater empfängt, dekodiert und sendet erneut – und zwar auf Kosten der Airtime, also der verfügbaren Sendezeit im Medium. Wer Repeater ohne Plan verteilt, kassiert halben Durchsatz, hohe Latenz und Roaming-Probleme, weil CSMA/CA, Hidden-Node-Effekte und Störungen gnadenlos zuschlagen. Repeater machen Sinn, wenn die Link-Bedingungen stimmen, der Backhaul clever gelöst ist und das Frequenzdesign passt. Repeater sind Werkzeuge, keine Wunderwaffen – und genau so solltest du sie einsetzen. Und ja: Repeater können fantastisch funktionieren, wenn du die Physik respektierst.

Bevor wir in die Tiefe gehen, legen wir die Begriffe sauber fest, denn „WLAN-Verstärker“ ist Werbung, kein Standard. Ein Repeater arbeitet Layer-2, empfängt Frames, verarbeitet sie und sendet sie weiter, was Half-Duplex-bedingt Airtime frisst. Ein klassischer „WLAN-Extender“ ist meist nichts anderes als ein Repeater mit hübscher Verpackung. Ein Mesh-Knoten kann wie ein Repeater arbeiten, nutzt aber idealerweise einen dedizierten Backhaul-Link, um die Bandbreiten-Kaskade zu vermeiden. Der Access Point mit Ethernet- oder PoE-Backhaul ist das goldene Kalb: maximale Stabilität, minimale Latenz, planbares Roaming. Repeater bleiben die Brücke, wenn du nicht überall Kabel legen kannst – aber dann bitte mit Plan.

Die wichtigste Regel im ersten Drittel dieses Artikels: Repeater sind kein Allheilmittel, Repeater dupeln keine Physik aus, Repeater brauchen ein gutes Eingangssignal, Repeater wollen dedizierten Backhaul, Repeater funktionieren nur im durchdachten Funkdesign. Wenn du Repeater richtig einsetzen willst,

reden wir über RSSI in dBm, über SNR in dB, über Modulationsstufen (MCS), über Kanalbreiten, DFS-Risiken, EIRP-Limits und darüber, wo du das Gerät tatsächlich aufstellst. Wer das ignoriert, skaliert Probleme statt Performance. Lass uns die Mythen zerlegen und danach ein Setup bauen, das wirklich trägt.

Was ein Repeater wirklich macht – Physik, Funk und Marketing-Bullshit erklärt

Ein Repeater ist kein Verstärker im analogen Sinn, sondern ein digitaler Regenerator auf Layer 2, der Frames empfängt, validiert und erneut aussendet. Das klingt trivial, kostet aber Airtime, weil WLAN half-duplex mittels CSMA/CA arbeitet und jedes Paket die Funkschnittstelle exklusiv belegt. Je schlechter das Eingangssignal, desto konservativer die Modulation (niedrigere MCS), desto länger dauert die Übertragung pro Bit, desto stärker schrumpft der nutzbare Durchsatz. Ein Repeater mit identischem Funkkanal für Front- und Backhaul halbiert die effektive Bandbreite typischerweise – und verschlimmert das bei mehreren Hops. Tri-Band-Geräte umgehen das, indem sie einen dedizierten 5-GHz- oder 6-GHz-Backhaul nutzen, der getrennte Airtime liefert. Das ist der Punkt, an dem Marketing recht hat: dedizierter Backhaul kann Repeater tauglich machen, ohne dein Netzwerk zu erdrosseln.

Die physikalische Basis ist das Linkbudget, also die Summe aus Sendeleistung, Antennengewinn, Freiraumdämpfung und Verlusten durch Wände, Decken und Möbel. In der Praxis arbeitest du mit RSSI in dBm und SNR in dB, denn aus beiden ergibt sich, welche MCS-Stufen stabil sind. Ein RSSI von etwa -60 bis -67 dBm am Repeater-Standort ist ein realistisches Fenster, um ausreichend hohe MCS zu fahren und trotzdem Reichweite zu verlängern. Ist das Eingangssignal schlechter (zum Beispiel -75 dBm), fällt der Repeater auf robuste, langsame Modulation zurück, was die gesamte Kette bremst. Die SNR sollte stabil über 20 dB liegen, denn Interferenzen durch Nachbar-WLANs, DECT, Mikrowellen oder Bluetooth senken die effektive Linkqualität. Kurz: Qualität rein, Qualität raus – oder eben nicht.

Auch Protokoll-Overhead ist real: Management-Frames, Retransmissions, Beacons, Block-Acks und die ganze 802.11-Party fressen Airtime, die du nicht siehst, aber bezahlen musst. Breitere Kanäle (80/160 MHz) sind nicht automatisch schneller, wenn das Störniveau hoch ist; oft performen 20/40 MHz stabiler, weil sie weniger kollidieren. DFS-Kanäle im 5-GHz-Band sind attraktiv, können aber bei Radarevents zu Kanalwechseln und Verbindungspausen führen. In 6 GHz entfällt DFS, dafür sind die Dämpfungsverluste höher, was Repeater-Positionierung noch sensibler macht. Beamforming, MU-MIMO und OFDMA helfen, aber nur, wenn Client, Repeater und AP sie sauber unterstützen – sonst bleiben sie Prospektlyrik. Verstehe das Protokoll, dann weißt du, warum dein Speedtest schwankt.

Repeater vs. Mesh vs. Access Point: die richtige Architektur für WLAN-Signalverlängerung

Ein klassischer Repeater kopiert Frames und funkt sie erneut – einfach, kostengünstig, aber nicht skalierbar. Mesh-Systeme bringen Routing-Intelligenz, Self-Healing und oft einen dedizierten Backhaul mit, was die größte Schwäche klassischer Repeater entspannt. Allerdings ist Mesh kein Freifahrtschein: Ohne dedizierten Backhaul oder mit zu vielen Hops landest du wieder bei halber Bandbreite pro Hop. Ein Access Point mit kabelgebundenem Backhaul (Ethernet, ideal via PoE) ist dagegen die Premiumlösung, weil Front- und Backhaul getrennt sind und die Funkzelle sauber geplant werden kann. Wenn du Zeit und Budget hast, verkable die Räume und setze APs – alles andere ist ein Kompromiss.

Architekturen entscheiden über Latenz, Roaming und Stabilität. Repeater neigen bei schlechter Planung zu hohen Latenzen, weil Frames mehrfach über das gleiche Medium gehen und Retransmissions zunehmen. Mesh mit dediziertem Backhaul halbiert die Zahl der Sorgen, wenn Kanäle koordiniert sind und die Sendeleistung pro Zelle reduziert wird, um Überlappungen zu kontrollieren. Access Points mit zentralem Controller (oder Cloud-Management) erlauben RRM, also automatische Kanal- und Leistungsoptimierung, was Airtime maximiert und Störungen minimiert. Wer also Gaming, VoIP oder Videokonferenzen ohne Aussetzer will, wählt bevorzugt APs mit Ethernet, akzeptiert Mesh mit dediziertem Backhaul – und nutzt Repeater sparsam, gezielt und datenbasiert. Alles andere ist würfeln.

Client-Verhalten ist der unterschätzte Faktor in jeder Architekturentscheidung. Viele Endgeräte halten hartnäckig an der ersten BSSID fest („Sticky Clients“), selbst wenn ein besserer AP oder Repeater nebenan ruft. Mesh-Systeme helfen mit 802.11k/v/r, also Nachbarschaftsberichten, Assisted Roaming und Fast BSS Transition, aber die Implementierung schwankt zwischen Herstellern. Repeater ohne Controller-Intelligenz liefern selten sauberes Roaming, was bei Bewegung im Haus zu Lags führt. Wer produktiv arbeiten muss, trennt SSIDs klug, setzt auf Band-Steering und limitiert Sendeleistung, um Zellen klar abzugrenzen. Gute Architektur ist die halbe Miete, die andere Hälfte ist Client-Realität, die du nicht ändern kannst – also plane drum herum.

Planung: Linkbudget, dBm, SNR

und Kanalwahl – so setzt du Repeater richtig ein

Planen heißt messen, nicht raten. Starte mit einer Site-Survey, selbst wenn es nur eine grobe Messung mit einer App wie WiFiman, AirPort Utility oder Wi-Fi Analyzer ist. Ermittle RSSI und Noise Floor in den Bereichen, in denen der Repeater stehen soll, und notiere SNR-Werte. Ziel ist ein RSSI am Repeater zwischen -60 und -67 dBm bei stabiler SNR über 20 dB, damit hohe MCS-Stufen genutzt werden. Miss über mehrere Zeitfenster, denn Interferenzen sind dynamisch und abhängig von Nachbarn, Mikrowellen und Belegung. Räume mit Stahlbeton, Fußbodenheizung oder gedämmten Wänden verhalten sich anders als Trockenbau – du brauchst reale Daten. Ohne Messung positionierst du Repeater blind, und blind fliegt selten gut.

Kanalplanung ist kein Kunsthandwerk, sondern Mathematik und Rücksichtnahme. Im 2,4-GHz-Band sind effektiv nur die Kanäle 1, 6 und 11 überlappungsfrei, also nutze exakt diese und setze die Sendeleistung niedrig, um Überreichweiten zu vermeiden. Im 5-GHz-Band hast du mehr Spielraum, aber DFS-Kanäle können Radaralarme auslösen, was bei Repeatern unschöne Hänger produziert; daher bevorzugt UNII-1/3, wenn die Umgebung es zulässt. In 6 GHz gibt es viel Platz, aber Reichweite ist schwächer, was den Repeater-Standort noch kritischer macht. Kanalbreiten von 80/160 MHz sind verlockend, aber nur sinnvoll, wenn die Umgebung leer ist; in Mehrfamilienhäusern sind 20/40 MHz oft überlegen. Koordiniere Kanäle zwischen Haupt-AP und Repeater, damit Backhaul und Client-Verkehr sich nicht gegenseitig überfahren.

Behalte EIRP-Grenzen und Regulatorik im Blick, sonst optimierst du dich illegal. In Europa gelten ETSI- und CE-Vorgaben, die die effektive isotrope Strahlungsleistung begrenzen; die Summe aus Sendeleistung und Antennengewinn zählt. Drehe nicht wahllos an der Leistung, denn hohe TX-Power macht zwar den Downlink lauter, der Uplink des Clients bleibt aber schwach – asymmetrische Links sind instabil. Besser ist es, mehrere Zellen mit geringerer Leistung zu bauen, die sich sauber überlappen. Teste die Platzierung iterativ: Stelle den Repeater zuerst dort auf, wo das Eingangssignal gut ist, dann überprüfe Downlink- und Uplink-Throughput mit iPerf3. So erkennst du Engstellen, bevor dich Nutzerfeedback trifft.

Installation und Konfiguration: Backhaul, Band-Steering, WPA3 – Schritt für

Schritt

Die Installation entscheidet über 80 Prozent des Ergebnisses, die restlichen 20 Prozent sind Feintuning. Nutze wo möglich Geräte mit dediziertem Backhaul (Tri-Band oder 6-GHz-Mesh), damit Front- und Backhaul sich nicht um Airtime prügeln. Richte identische SSID und Security zwischen Haupt-AP und Repeater ein, aber lass den Repeater nicht blind die Kanäle kopieren – plane sie. Aktiviere WPA3-Personal, sofern alle Clients das unterstützen, andernfalls WPA2/WPA3-Transition, aber nimm niemals WEP oder offene Netze. Schalte WPS ab, weil es Angriffsfläche schafft und Stabilität kostet. Stell die Sendeleistung moderat ein, damit Clients nicht an zu lauten, aber weit entfernten Zellen hängen bleiben. Mit Band-Steering verschiebst du geeignete Clients ins 5- oder 6-GHz-Band, wo mehr Platz ist.

Roaming-Optimierung ist eine Mischung aus Standards und Reality-Check. Aktiviere 802.11k/v, damit Clients Nachbarschaftsinformationen bekommen, und 802.11r, wenn du viele Voice- oder Echtzeitanwendungen hast. Setze Minimum Data Rates so, dass sehr langsame Clients nicht die Airtime verbrennen; deaktiviere MCS 0–1, wenn es die Umgebung zulässt. Prüfe die Beacon-Intervalle und DTIM-Werte, um Energiesparen nicht gegen Latenz auszuspielen. Nutze VLANs für Gastnetze mit Client Isolation, damit Smart-Home-Spielzeug nicht dein Arbeitsgerät sieht. Wenn möglich, trenne IoT mit 2,4 GHz von produktiven Geräten mit 5/6 GHz, um Airtime-Konkurrenz zu reduzieren. Gute Defaults sparen dir später viel Troubleshooting.

- Standort wählen: Ziel-RSSI am Repeater zwischen -60 und -67 dBm messen
- Backhaul planen: dediziertes 5/6-GHz-Band oder Ethernet, keine geteilte Airtime, wenn möglich
- Kanal und Breite festlegen: 2,4 GHz nur 1/6/11, 5 GHz bevorzugt UNII-1/3, Breite nach Störlage
- Sicherheit aktivieren: WPA3 oder WPA2/WPA3-Transition, WPS aus, starke Passphrase
- Leistung justieren: moderate TX-Power, um saubere Zellgrenzen und besseres Roaming zu fördern
- Band-Steering einschalten: Clients in 5/6 GHz ziehen, wo es sinnvoll ist
- Roaming-Standards: 802.11k/v/r aktivieren, Minimum Rates anpassen
- Gastnetz und VLAN: Trennung für Sicherheit und Netzwerkhygiene
- Firmware updaten: aktuelle Treiber und Bugfixes sind Performance-Faktoren
- Abschlussmessung: iPerf3, Ping-Jitter und Packet Loss dokumentieren

Leistung messen und optimieren: Tools, iPerf,

Spektrumanalyse und Roaming

Wer nicht misst, irrt im Kreis und diskutiert über Gefühle. Starte mit iPerf3 für Throughput in beide Richtungen: Downlink, Uplink und bidirektional mit parallelen Streams, um Engpässe sichtbar zu machen. Ergänze Latenz- und Jitter-Messungen via Ping und if möglich VoIP-MOS-Simulation, damit du nicht nur Peaks, sondern Stabilität bewertest. Nutze einen Spektrumanalysator oder Apps mit Spektrum-Sicht, um Non-Wi-Fi-Interferenzen zu erkennen; viele Probleme kommen nicht vom Nachbar-WLAN, sondern von Mikrowellen, Funkkameras oder defekten Netzteilen. Lighthouse und Speedtest sind für Internet-Ende nett, aber für WLAN-Bewertung sekundär; lokal ist König, Internet ist Zubringer. Dokumentiere Messpunkte auf einem Grundriss – Papier reicht –, damit Änderungen nachvollziehbar bleiben.

Airtime ist die Währung, also optimiere sie. Reduziere Broadcast- und Multicast-Verkehr, indem du IGMP Snooping aktivierst und unnötige Protokolle abstellst. Deaktiviere Legacy-Raten, die nur Ballast sind, und halte die Anzahl der SSIDs klein; jede SSID erzeugt Beacons und frisst Airtime. Prüfe Retransmission- und Retry-Raten im Controller oder mit Sniffer, um Störungen von Coverage-Problemen zu unterscheiden. Wenn Retries hoch sind, sind SNR oder Interferenzen schlecht; wenn Client-Rate konstant niedrig ist, ist es eher ein Coverage- oder MCS-Thema. Bei viel IoT entlaste 2,4 GHz durch konsequente Kanalplanung und minimale Leistung – weniger Reichweite, weniger Kollisionen. Kleine Stellschrauben summieren sich zu großer Wirkung.

Roaming testest du nicht am Schreibtisch, sondern im Gang. Gehe mit einem Endgerät durch die Räume, logge RSSI, BSSID und Latenz und beobachte, wie schnell die Übergabe erfolgt. Bei Verzögerungen prüfe 802.11r-Kompatibilität der Clients, denn einige ältere Geräte zicken bei FT. Setze Roaming-Thresholds behutsam, sonst lösen Clients zu früh aus und pendeln. Wenn du Mesh nutzt, überwache Backhaul-Qualität und Hop-Distanzen; ein Knoten mit schlechtem Backhaul ist ein Bremsklotz, egal wie gut seine Front-Clients stehen. Und wenn alles nichts hilft, ziehe ein Ethernet-Kabel – jedes echte Backhaul spart dir Stunden Lebenszeit.

Repeater im 5G- und IoT-Kontext: Mobilfunk-, LoRa- und Outdoor-Szenarien

Repeater existieren nicht nur im WLAN, sondern auch im Mobilfunk – und da wird es rechtlich heikel. In Deutschland sind aktive Mobilfunk-Repeater ohne Betreiberzustimmung in der Regel nicht zulässig, die Bundesnetzagentur versteht da keinen Spaß. Wer Indoor-Mobilfunk verbessern will, nutzt vom Netzbetreiber freigegebene Repeater, Small Cells oder Femto-/Picozellen, die am Core registriert sind. Für 5G NR gibt es intelligente Repeater, die bestimmte Bänder verstärken und digitale Filter nutzen, aber auch hier gilt:

nur mit Genehmigung und sauberem Setup. Alternativ: nutze eine 5G-CPE am Fenster und verteile das LAN intern via APs oder Mesh mit dediziertem Backhaul. Illegaler Mobilfunk-Repeater-Einsatz stört ganze Zellen – und endet teuer.

Im IoT-Bereich sieht die Welt anders aus, weil Protokolle wie LoRaWAN, Zigbee oder Thread andere Reichweiten- und Topologie-Modelle haben. LoRa arbeitet mit extrem schmaler Bandbreite und hoher Empfindlichkeit, sodass Repeater selten nötig sind; stattdessen setzt man zusätzliche Gateways mit Ethernet-Backhaul. Zigbee kann Mesh nativ, wobei „Router“-Knoten die Rolle von Repeatern übernehmen; zu viele Hops erhöhen aber Latenz und Paketverlust. Thread (Basis für Matter) bringt IP-basiertes Mesh mit, was stabiler ist, solange genug Router-Knoten vorhanden sind. Für Outdoor-WLAN setze statt Repeatern auf Richtfunk- oder PtP-Links (5/60 GHz) mit sauberem Linkbudget, dann Access Points vor Ort. Repeater sind das Werkzeug, wenn Kabel unmöglich ist, nicht die Standardlösung.

Spezialfall Campus oder Lagerhalle: Hier verbrennen Repeater oft nur Airtime, weil Metallregale, Maschinen und Flurfahrzeuge die Funksituation permanent ändern. Besser sind mehrere APs mit industrietauglichen Antennen (Sektor, Panel), zentralem Controller und sauberer Kanalplanung. Wenn dennoch Repeater nötig sind, dann mit dediziertem Backhaul und klar begrenzten Zellen. Plane Wartungswege für Firmware-Updates, denn Sicherheitslücken in Funkgeräten sind keine Theorie. Und ja, setze auf robuste Stromversorgung – eine Powerline-Fantasie ist kein Backhaul, sondern Latenz mit Marketingdeckel.

Sicherheit, Compliance und Troubleshooting: Recht, ETSI, DFS und die üblichen Fehler

Sicherheit beginnt bei Basics, die erschreckend oft ignoriert werden. Deaktiviere WPS konsequent, nutze WPA3 wo möglich und sichere das Management-Interface deines Repeaters mit starken Passwörtern und Updates. Trenne Netze logisch per VLAN und setze Client Isolation in Gastnetzen, um East-West-Verkehr zu unterbinden. Halte Firmware aktuell, denn Treiber- und Stack-Bugs sind Performance- und Sicherheitskiller zugleich. Prüfe die Hersteller-Roadmap: Geräte ohne Update-Politik sind Elektroschrott mit Wartezeit. Logging ist Pflicht, nicht Kür – ohne Logs lässt sich nichts sauber analysieren.

Compliance ist kein „Vielleicht“, sondern der Rahmen, in dem du arbeiten darfst. Achte auf CE-Kennzeichnung, ETSI-Konformität und die richtige Länderkennung, damit Kanäle, Leistung und DFS korrekt greifen. Static-DFS-Hacks und falsche Ländereinstellungen mögen kurzfristig Speed bringen, aber sie sind illegal und zerstören Nachbarschaftsnetze. In Mobilfunknetzen gilt: Finger weg von nicht genehmigten Repeatern, alles andere klärst du mit dem Netzbetreiber. Dokumentiere dein Setup, inklusive Kanälen, Leistung und Standorten – das schützt dich im Zweifel und hilft bei der Optimierung. Wer

Regeln ignoriert, verliert erst Performance, dann Nerven und am Ende Geld.

Fehlerbilder wiederholen sich, also kenne sie. Doppel-NAT durch Repeater mit eigenem Routermodus sorgt für kaputtes Port-Forwarding und VPN-Probleme – nutze Bridge-Modus. Hohe Latenzspitzen deuten auf Airtime-Sättigung hin, nicht auf schlechte Leitung; prüfe Retries, Kanalbreite und SSID-Anzahl. Hidden-Node-Effekte entstehen, wenn Clients sich gegenseitig nicht sehen, aber mit demselben AP sprechen – kleinere Zellgröße und Leistungslimits helfen. DFS-Events reißen Verbindungen ab: Wenn kritisch, vermeide DFS-Kanäle. Bufferbloat killt Echtzeitdienste; aktiviere SQM/Smart Queue Management am Gateway. Und wenn ein Repeater ständig die Verbindung verliert, ist der Standort schlecht – nicht die Welt gegen dich.

Fazit: Repeater mit Verstand statt Hoffnung

Repeater sind weder Teufelszeug noch Zauberstab, sie sind Werkzeuge mit harten Grenzen. Wer Repeater richtig einsetzen will, plant Funkzellen, misst Signale, achtet auf SNR und MCS, wählt Kanäle bewusst und sorgt für einen Backhaul, der Frontverkehr nicht ausbremst. Mit dedizierten Backhaul-Bändern, sauberer Kanalplanung, moderater Leistung und WPA3 liefern Repeater solide Ergebnisse. Ohne das ist es ein Glücksspiel mit halber Bandbreite, hoher Latenz und Frust im Alltag. Die Physik gewinnt immer – arbeite mit ihr, nicht gegen sie.

Wenn du stabile Reichweite willst, ist Verkabeln mit Access Points die Königsdisziplin, Mesh mit dediziertem Backhaul der taugliche Plan B und der Repeater die pragmatische Brücke. Messen schlägt Meinen, und Dokumentation schlägt Bauchgefühl. Respektiere Regulatorik, halte Firmware frisch, minimiere SSIDs und manage Airtime, dann bleibt das Netzwerk leise, schnell und zuverlässig. Und wenn alles wackelt: Kabel ziehen, iPerf3 laufen lassen, dann repeat. Genau so meisterst du Signalverlängerung clever – nicht mit Hoffnung, sondern mit Technik.