

Kritische Entra-ID-Lücke machte alle Tenants global kompromittierbar

Aufgrund einer Schwachstelle in Entra ID hätten Angreifer als Admin auf beliebige Tenants zugreifen können. Das Sicherheitsproblem ist schon länger gelöst.



32



(Bild: RaiDztor/Shutterstock.com)

19.09.2025, 10:36 Uhr Lesezeit: 2 Min. | Security

Von Dennis Schirrmacher

Microsofts Identitäts- und Zugriffsverwaltungsdienst Entra ID war kaputt. Angreifer hätten mit vergleichsweise wenig Aufwand an einer "kritischen" Sicherheitslücke ansetzen können. Davon waren global alle Entra-ID-Tenants betroffen. Microsoft hat die Schwachstelle im Juli dieses Jahres geschlossen. Nun führt ein Sicherheitsforscher Hintergründe zur Lücke aus.

1 Jahr mit 50 % Rabatt

Rabatt sichern

Durch das erfolgreiche Ausnutzen der Schwachstelle war ein Admin-Zugriff auf beliebige Tenants möglich. Weil weltweit unter anderem große Unternehmen Entra ID nutzen, hätten Attacken weitreichende Folgen haben können.

Hintergründe

In einem ausführlichen Beitrag erläutert ein Sicherheitsforscher von Outsidersecurity das Sicherheitsproblem. Er gibt an, die "kritische" Schwachstelle (CVE-2025-55241) mit Höchstwertung (CVSS Score 10 von 10) im Juli dieses Jahres entdeckt und umgehend an Microsoft gemeldet zu haben. Er schreibt, dass Microsoft die Schwachstelle innerhalb weniger Tage geschlossen hat. Dafür mussten Entra-ID-Tenants nichts tun. Offensichtlich wurde das Problem serverseitig gelöst.

Um die Lücke auszunutzen, mussten Angreifer aber die Tenant-ID und die NetID eines Nutzers kennen. Doch beides lässt sich dem Forscher zufolge mit vergleichsweise wenig Aufwand herausfinden. Dass das keine so große Hürde sein kann, unterstützt auch die kritische Einstufung der Schwachstelle.



Rabatt sichern

Dem Sicherheitsforscher zufolge fußt eine Attacke auf zwei Grundlagen: Der erste Ansatzpunkt ist ein undokumentierter Token zur Identitätsfeststellung mit der Bezeichnung "Actor Token". Diesen nutzt Microsoft in seinem Backend für Service-to-Service-Kommunikation.

Die zweite Komponente ist die eigentliche Schwachstelle in der Azure AD Graph API (Legacy), die solche Tokens nicht ausreichend überprüft. Demzufolge hätten sich Angreifer damit ausgerüstet als Admin für beliebige Tenants ausgeben können. Der Sicherheitsforscher führt aus, dass diese Tokens aufgrund ihrer Beschaffenheit an allen Sicherheitsrichtlinien vorbeischlüpfen, sodass es keine Gegenmaßnahme gab.

Nach erfolgreichen Attacken hätten Angreifer vollen Zugriff auf Entra-ID-Tenants gehabt. So hätten sie unter anderem persönliche Informationen und BitLocker-Schlüssel einsehen und die volle Kontrolle über Services wie SharePoint Online erlangen können. Erschwerend kommt hinzu, dass ein Angreifer mit einem Actor Token keine Spuren in Logs hinterlässt.

Videos by heise

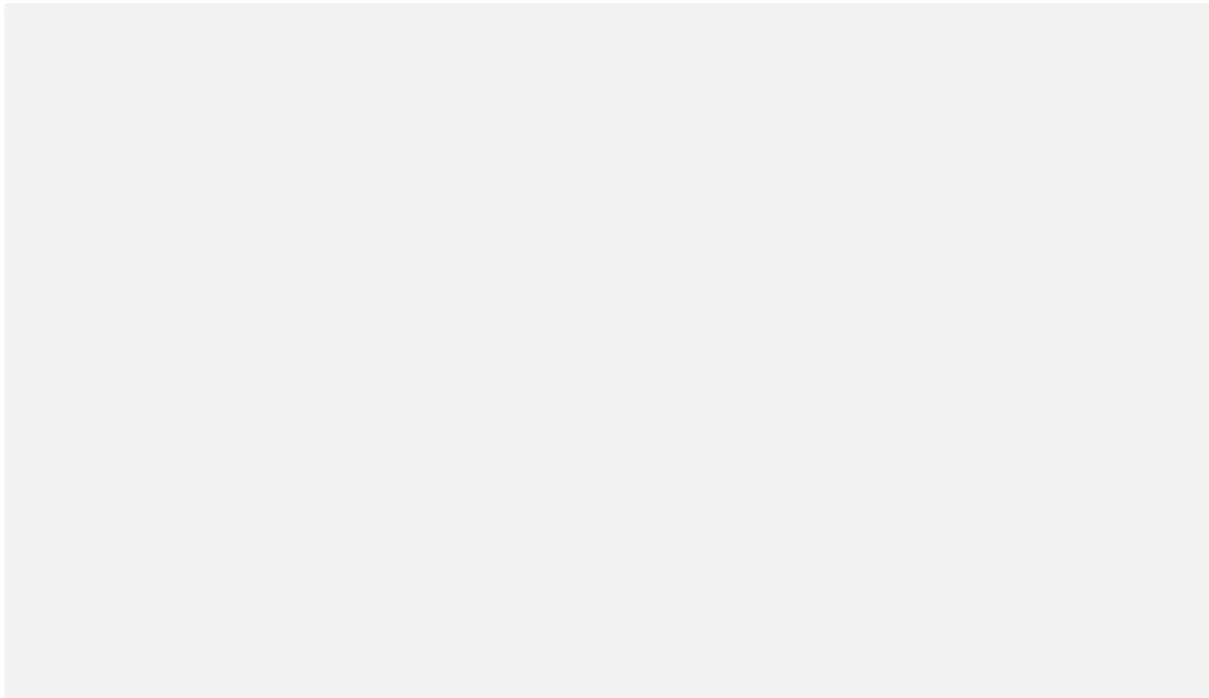
mehr Videos 

 1 Jahr mit 50 % Rabatt 

Rabatt sichern



Microsoft gibt an, dass ihnen keine derartigen Attacken bekannt sind. Der Sicherheitsforscher führt in seinem Bericht weitere technische Hintergründe aus. In einer Warnmeldung listet Microsoft weitere Details auf.



(des)

Kommentare lesen (32)

1 Jahr mit 50 % Rabatt

Rabatt sichern

[Zur Startseite](#)

Security Newsletter

Ob Sicherheitslücken, Viren oder Trojaner – alle sicherheitsrelevanten Meldungen gibts bei heise security

[Jetzt anmelden](#)

Ausführliche Informationen zum Versandverfahren und zu Ihren Widerrufsmöglichkeiten erhalten Sie in unserer Datenschutzerklärung.

 1 Jahr mit 50 % Rabatt 

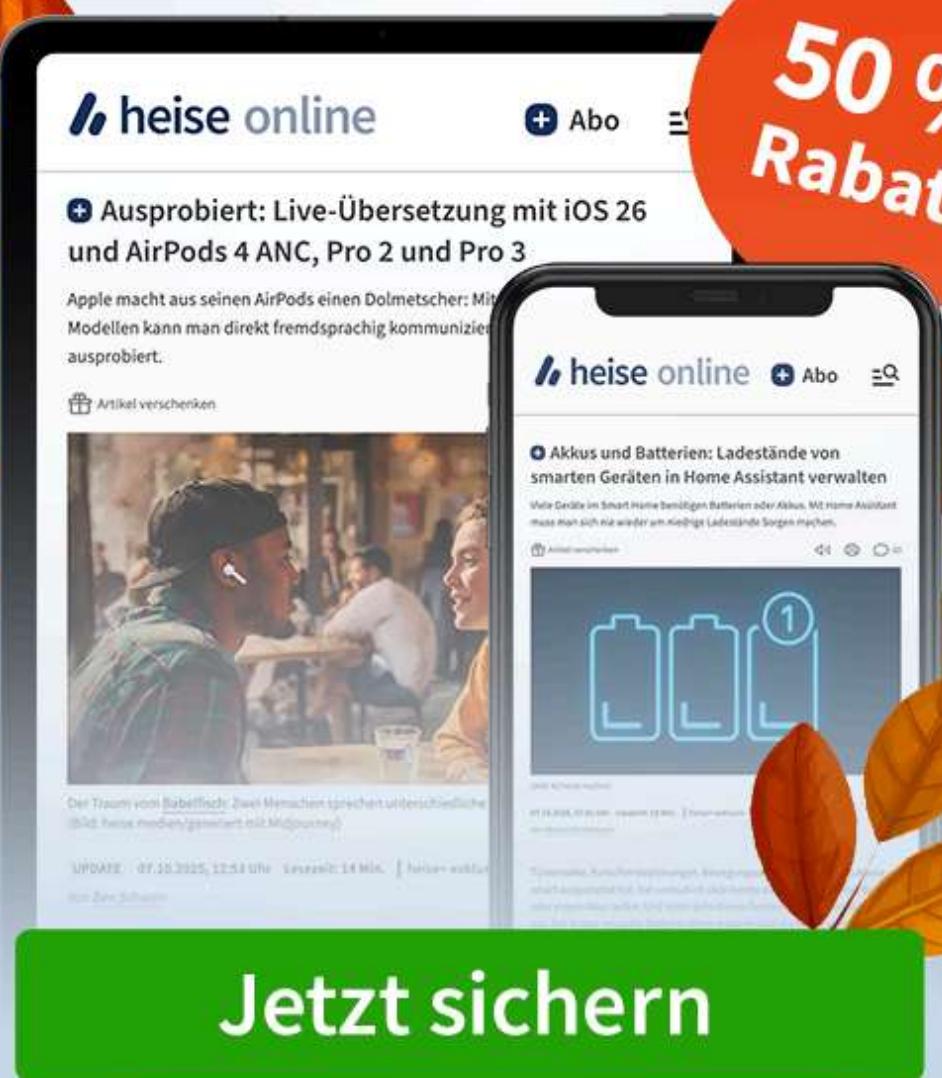
[Rabatt sichern](#)

Anzeige

WISSEN, DAS BLEIBT

1 Jahr **heise+**
zum halben Preis

50 %
Rabatt



heise online + Abo ⌂

Ausprobiert: Live-Übersetzung mit iOS 26 und AirPods 4 ANC, Pro 2 und Pro 3

Apple macht aus seinen AirPods einen Dolmetscher: Mit diesen Modellen kann man direkt fremdsprachig kommunizieren. Ausprobiert.

Artikel verschenken



Der Traum vom Babelfisch: zwei Menschen sprechen unterschiedliche Sprachen miteinander (Bild: Renzo Medrano/panoramio.com)

UPDATE: 07.11.2025, 12:51 Uhr | Lesezeit: 14 Min. | heise+ erfordert kein Zuhause

Jetzt sichern

+ 1 Jahr mit 50 % Rabatt 

Rabatt sichern

MEHR ZUM THEMA

Immer informiert bleiben: Klicken Sie auf das Plus-Symbol an einem Thema, um diesem zu folgen. Wir zeigen Ihnen alle neuen Inhalte zu Ihren Themen.

[Mehr erfahren.](#)

[Entra ID](#)

[IT](#)

[Microsoft](#)

[Security](#)

[Sicherheitslücken](#)

TEILE DIESEN BEITRAG



Kurzlink: <https://heise.de/-10662375>

Weitere Empfehlungen

Experte macht düstere Prognose: Kommt jetzt das...

Hausfrage



Testbericht: Wie gut ist Anti-Schädlings-Gerät wirklich? Da...

Verbraucherschutz



Vor dem aus? Warum sich Solar bald nicht mehr...

Hausfrage



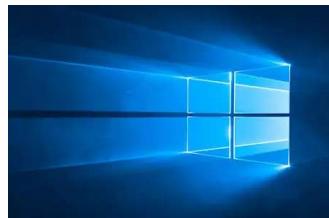
EU-Regeln kommen: Ohne Solaranlage wird's ab 2026...

Solar Aktuell | Checkfox



iOS warnt vor langsamen...

heise online



Festplatte klonen unter Windows ...

tipps + tricks



Windows-11-Key auslesen – so...

tipps + tricks



Windows 10 22H2: Update außer d...

heise online

1 Jahr mit 50 % Rabatt

Rabatt sichern

Anzeige



Anzeige

Nach Laura Dahlmeiers Tod: Tragische neue...

Merkur

Anzeige



Verluste im Ukraine-Krieg: Heikler Bericht z...

Frankfurter Rundschau

Anzeige



Vorsicht Autofahrer: Eine Radarfalle kann mehr a...

CHIP News

Zimmermädchen im Hotel verrät: Es bringt nichts,...

FOCUS Online - Reisen



Windows 11: Altes Kontextmenü...

tipps + tricks



Telekom und Vodafone müssen...

heise online



Mit Batterien aus alten E...

heise online



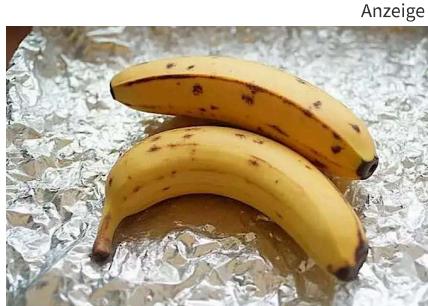
Amazon-Lieferdrohne...

heise online



Milben nisten sich unbemerkt im Bett ei...

Med Direkt



Schlechter Stuhlgang bei Senioren: Diesen...

Floravia



Baden-württemberg beschließt neues...

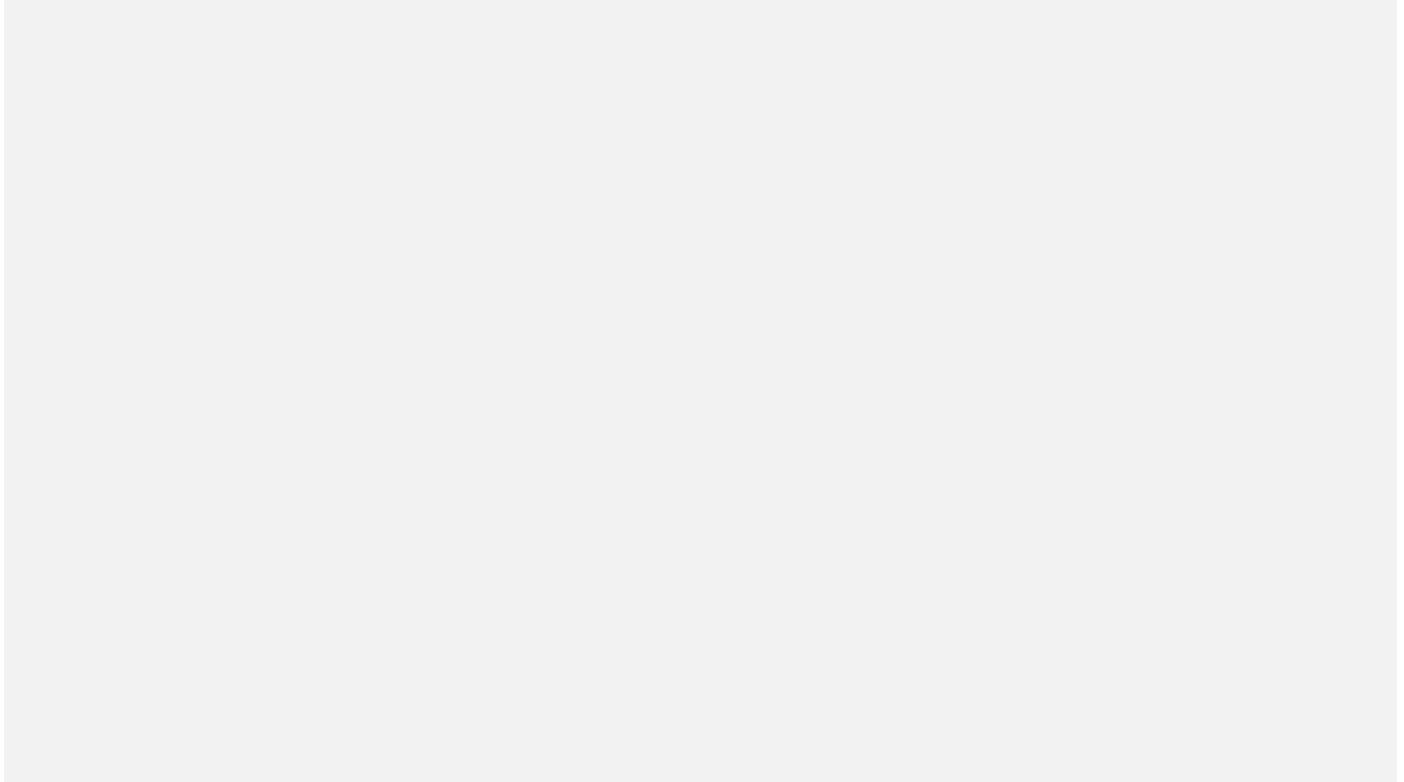
1komma5.com

Top-Beiträge von heise online

»

+ 1 Jahr mit 50 % Rabatt

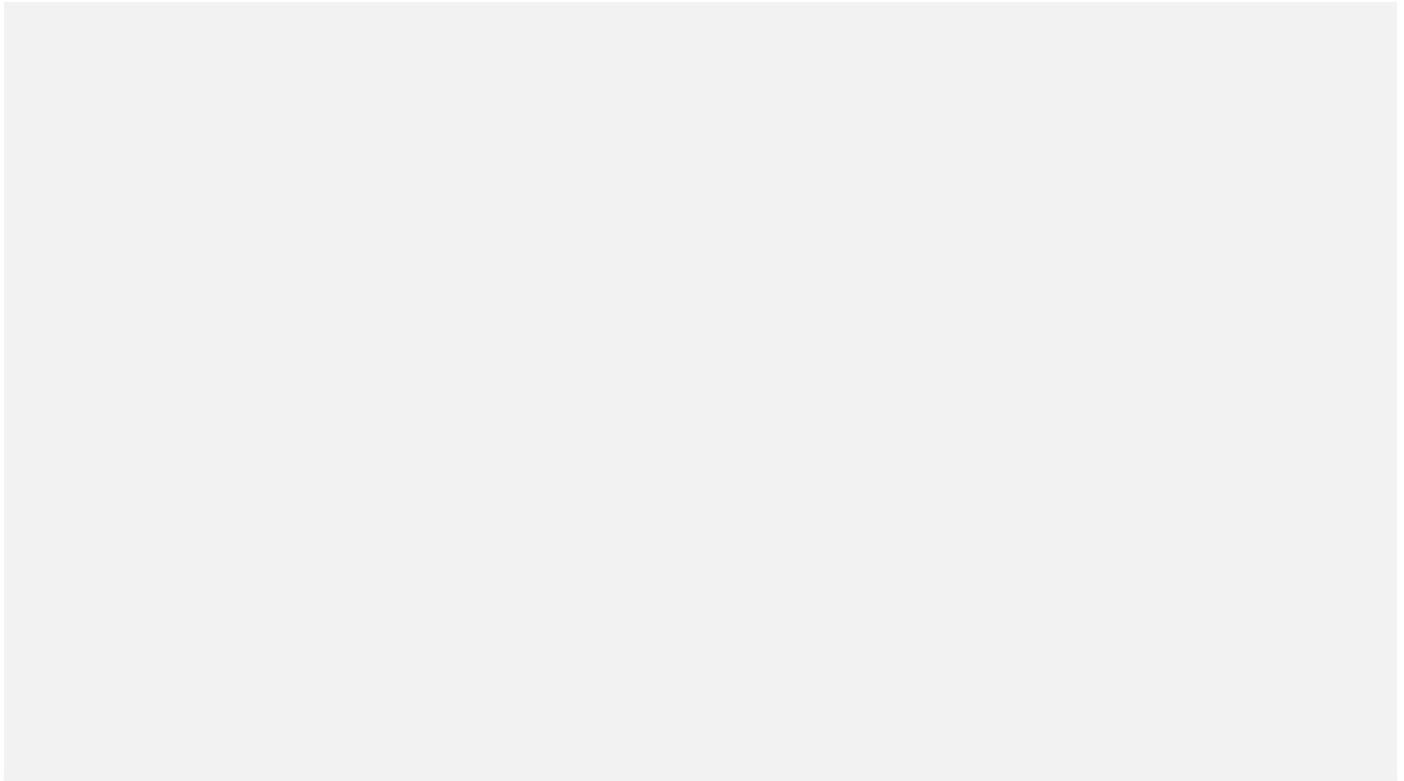
Rabatt sichern



News

Fast zwei Millionen Elektroautos auf der Straße

Die Zahl ist deutlich gestiegen, noch vor Jahresende könnte die Zwei-Millionen-Schwelle erreicht werden. Von früheren Plänen sind die Zahlen aber weit entfernt.



 1 Jahr mit 50 % Rabatt 

Rabatt sichern

Nach der Zerschlagung eines Cybercrime-Netzwerks erklären wir, wie die Täter genau vorgingen und was Verbraucher wissen und worauf sie achten sollten.

News

Apples iPhone-Geschäft läuft gut – aber welches kaufen?

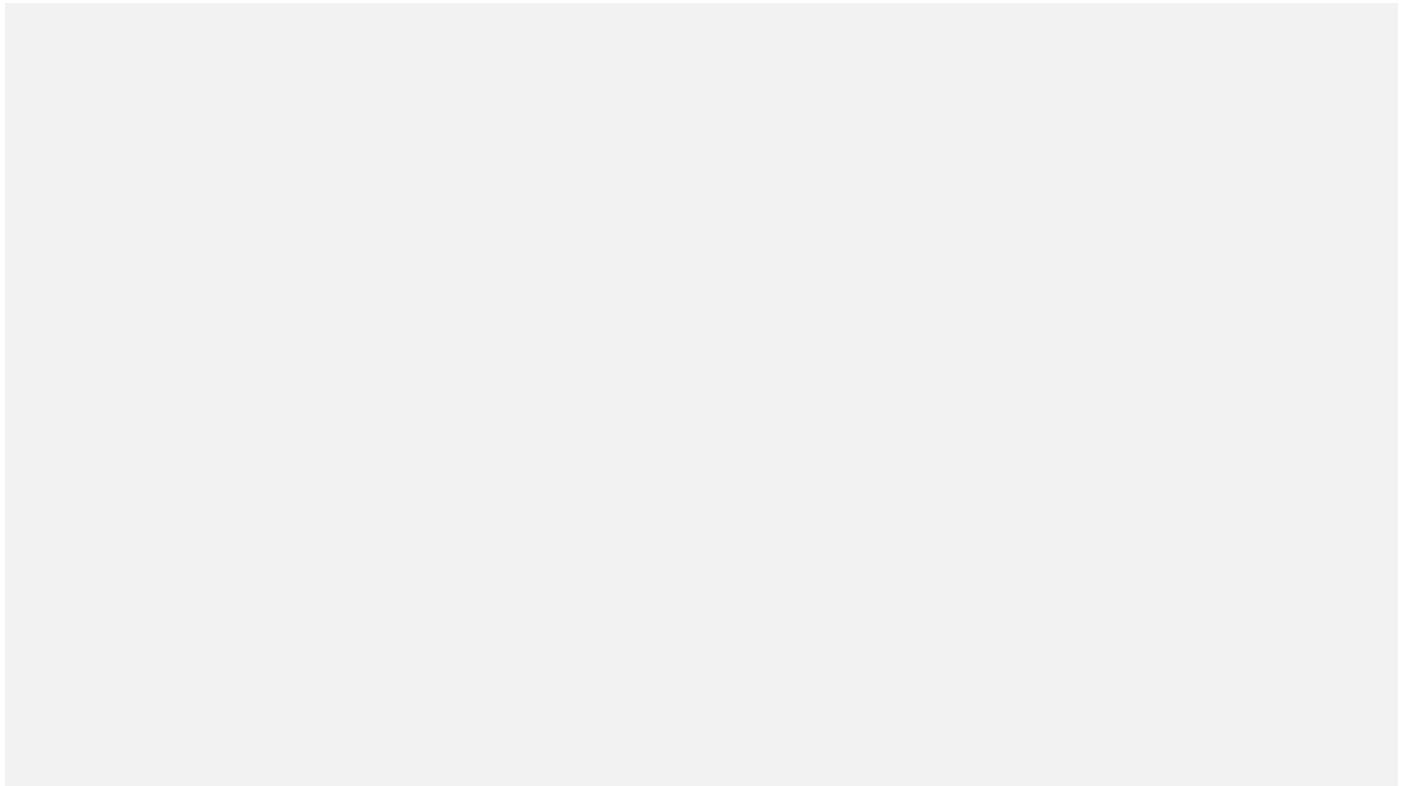
Apple erwartet zum Weihnachtsgeschäft die bislang besten iPhone-Verkäufe aller Zeiten. Für Käufer wird es aber immer unübersichtlicher.

 1 Jahr mit 50 % Rabatt 

Rabatt sichern

US-Patentamt ändert Regeln für KI-gestützte Erfindungen

Das US-Patentamt hat festgelegt, wie mithilfe von KI entwickelte Erfindungen gewerblich geschützt werden können. Eine natürliche Person muss im Spiel sein.



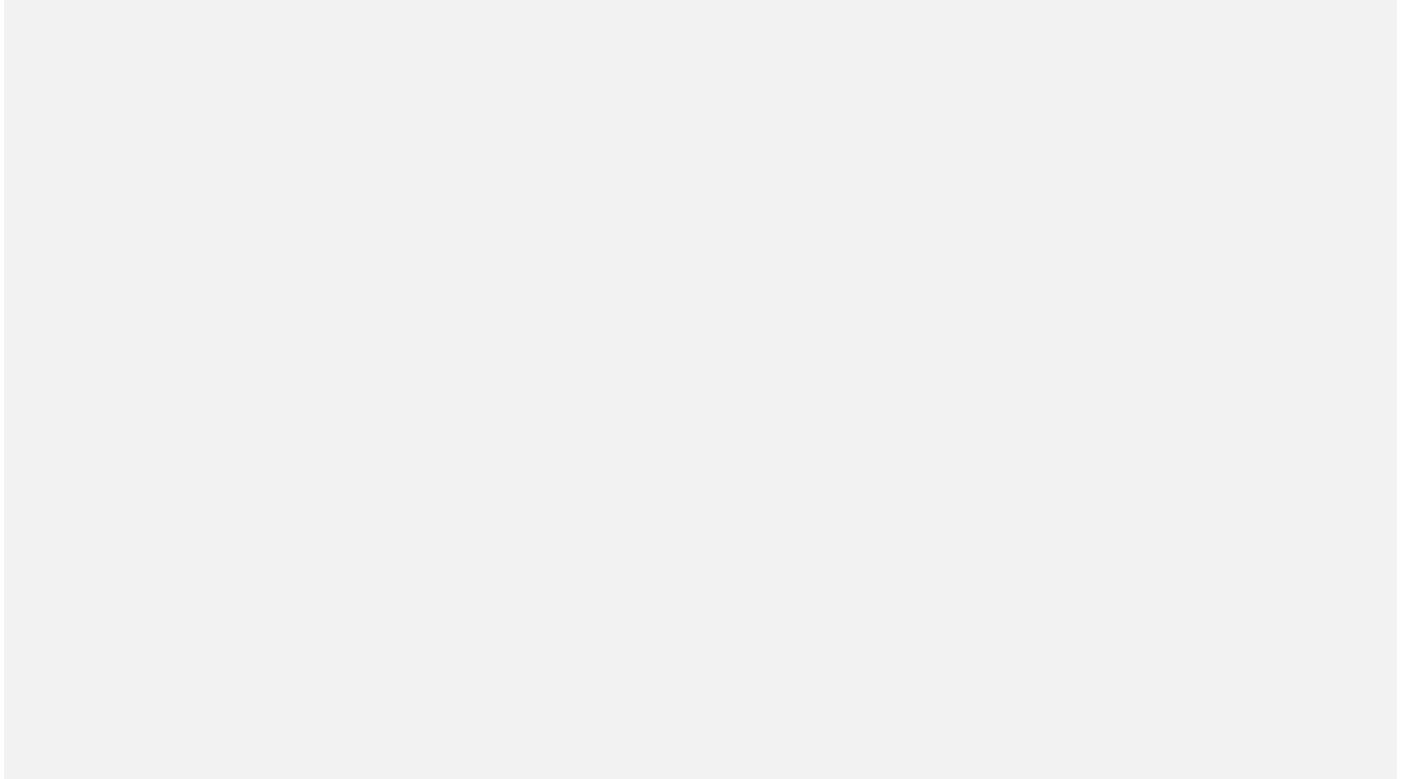
Hintergrund

+ Bahn-Chaos und Verspätungen: Warum die Sanierung der Gleise allein nicht hilft

Überall wird bei der Bahn gebaut. Doch an vielen Problemen des Schienennetzes ändert das langfristig wenig. Warum das so ist und was man besser machen könnte.



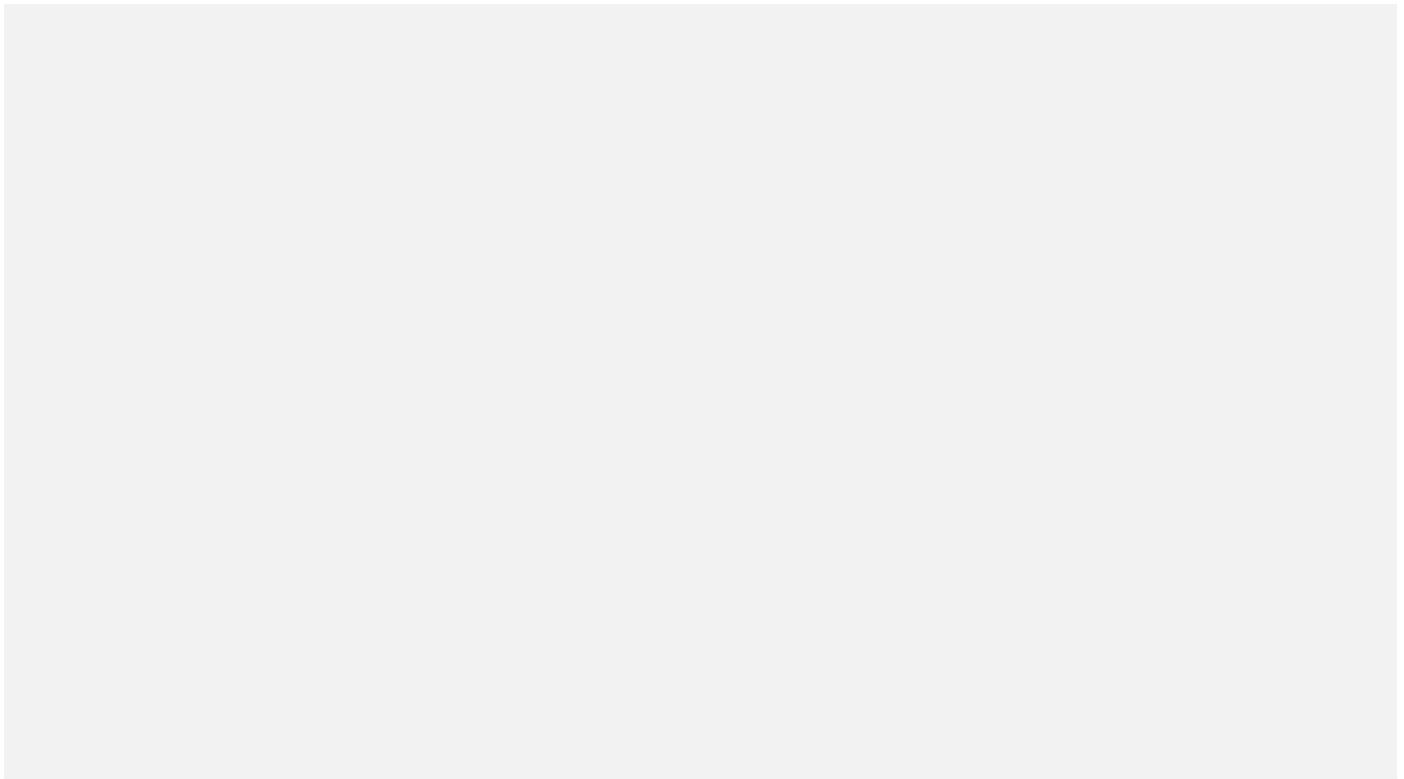
Rabatt sichern



Ratgeber

Vorsicht, Kunde: Keine Gewährleistung ohne Video bei Drogeriemarkt Müller

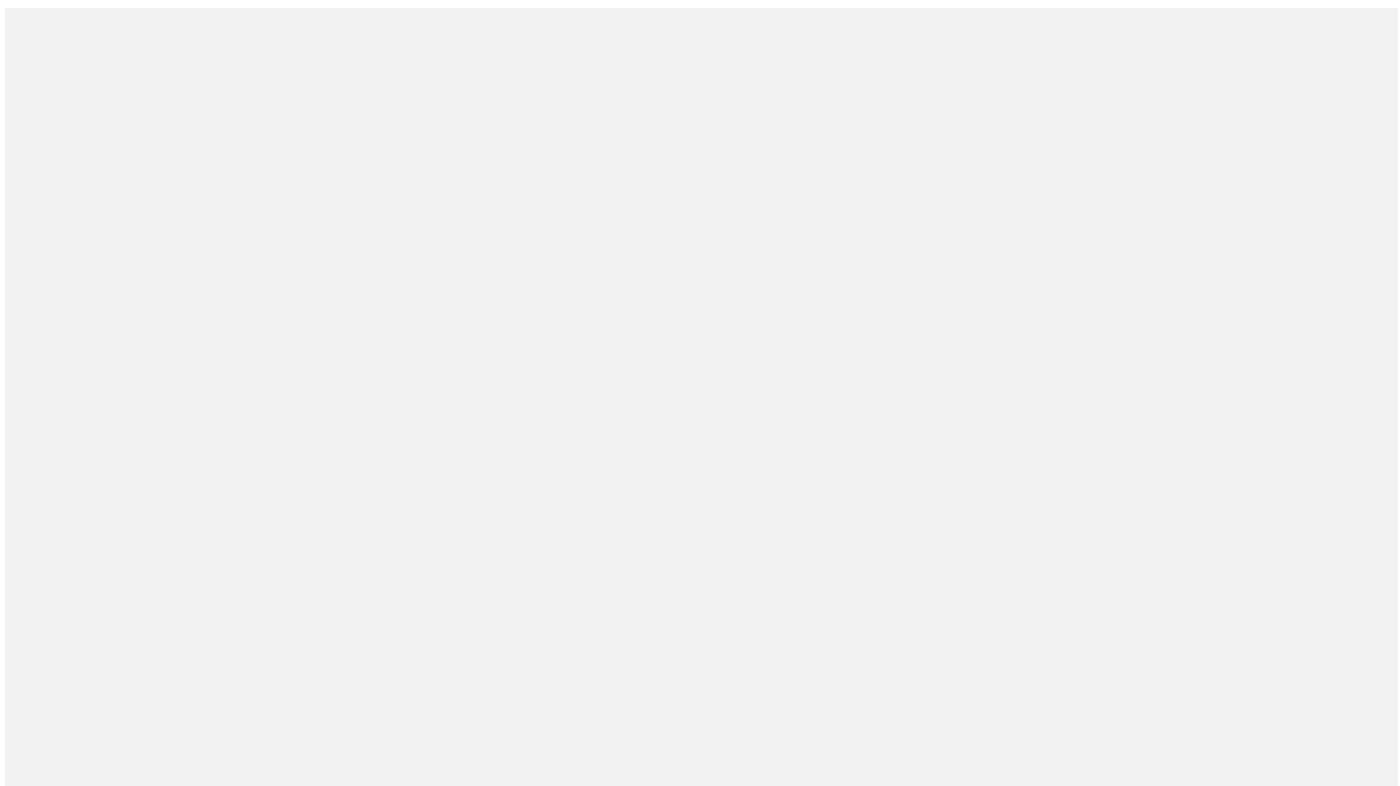
Der Onlineshop mueller.de will Reklamationen nur prüfen, wenn der Kunde ein Video per E-Mail einsendet. Doch das scheitert schon an den Volumenbeschränkungen.



 **1 Jahr mit 50 % Rabatt** 

Rabatt sichern

Wero ist im Onlinehandel gestartet. Wir geben einen aktuellen Überblick zum Stand des europäischen Bezahlsystems und haben es im Shop ausprobiert.



News

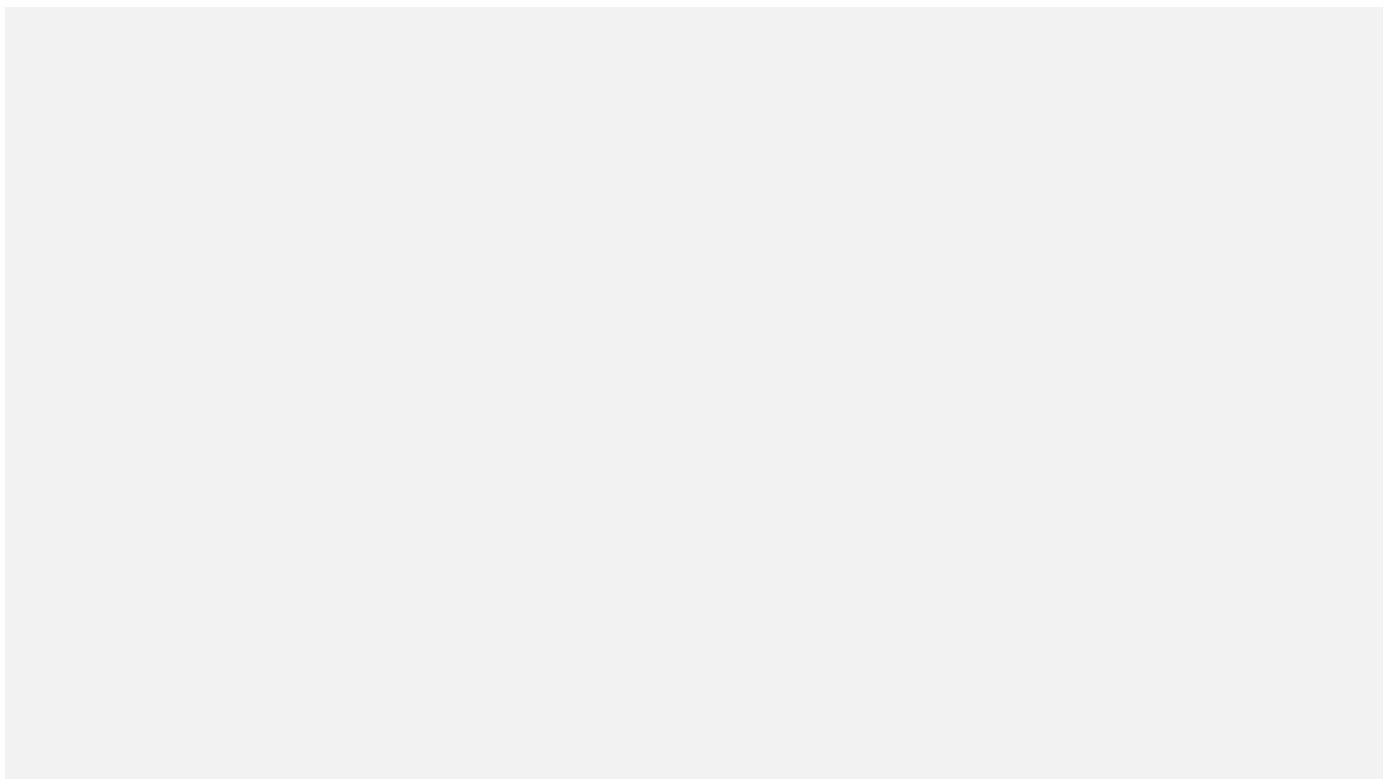
Raspberry-Pi-Projekte fürs Netz – NAS, Cloud & Router selbst gebaut | c't uplink

Der Raspberry Pi eignet sich für vieles: Opencloud-Host, Selbstbau-NAS oder als OpenWRT-Router. Die Vorteile davon und wie das geht, erklären wir in c't uplink.

Beliebte Bestenlisten

 1 Jahr mit 50 % Rabatt 

Rabatt sichern



Letzte Chance für Top-Angebote zum Finale der Black Week

bestenlisten

Weder Apple noch Nintendo: Die beliebtesten Black-Friday-Deals

bestenlisten

Die besten Black-Friday-Angebote für Laptops & Mini-PCs

bestenlisten

Alle bestenlisten →

1 Jahr mit 50 % Rabatt

Rabatt sichern

Alle Angebote

IT News

Newsticker

Hintergründe

Ratgeber

Tests

Meinungen

Online-Magazine

heise+

Telepolis

heise autos

bestenlisten

tipps+tricks



1 Jahr mit 50 % Rabatt

Rabatt sichern

[heise shop](#)[heise jobs](#)[heise academy](#)[heise download](#)[heise preisvergleich](#)[Tarifrechner](#)[heise compaliate](#)[Abo bestellen](#)[Mein Abo](#)[Netzwerktools](#)[iMonitor](#)[Loseblattwerke](#)[Spiele](#)

Über Uns

[heise medien](#)[heise regioconcept](#)[heise business services](#)[Sponsoring !\[\]\(8666c9b3547f1b159cfa188cdad63d82_img.jpg\)](#)[Mediadaten](#)[Karriere](#)[Presse](#)[!\[\]\(7349b8cb1ec6d06b56c460cf745b37fb_img.jpg\) Newsletter](#) [!\[\]\(444041ad754ee9ad3f932c8d708e23f5_img.jpg\) heise-Bot](#) [!\[\]\(c3d207c4dc9c22e1f1c2687804a231eb_img.jpg\) Push](#)[!\[\]\(2cc16dd33438b13a81598d17a56fea4b_img.jpg\) nach oben](#)[Kontakt](#)[Impressum](#)[Barriere melden](#)[Verträge kündigen](#)[Cookies & Tracking](#)[Datenschutz](#)[Mediadaten](#)

4941449

Content Management by InterRed

Hosted by Plus.line

[!\[\]\(204341496d4e729ec750b610c6816327_img.jpg\) 1 Jahr mit 50 % Rabatt !\[\]\(86b5d6a2f21bffd988334588d0f8f172_img.jpg\)](#)[Rabatt sichern](#)

**+ 1 Jahr mit 50 % Rabatt** 

Rabatt sichern