## KSV Fuchs | F. Fuchs

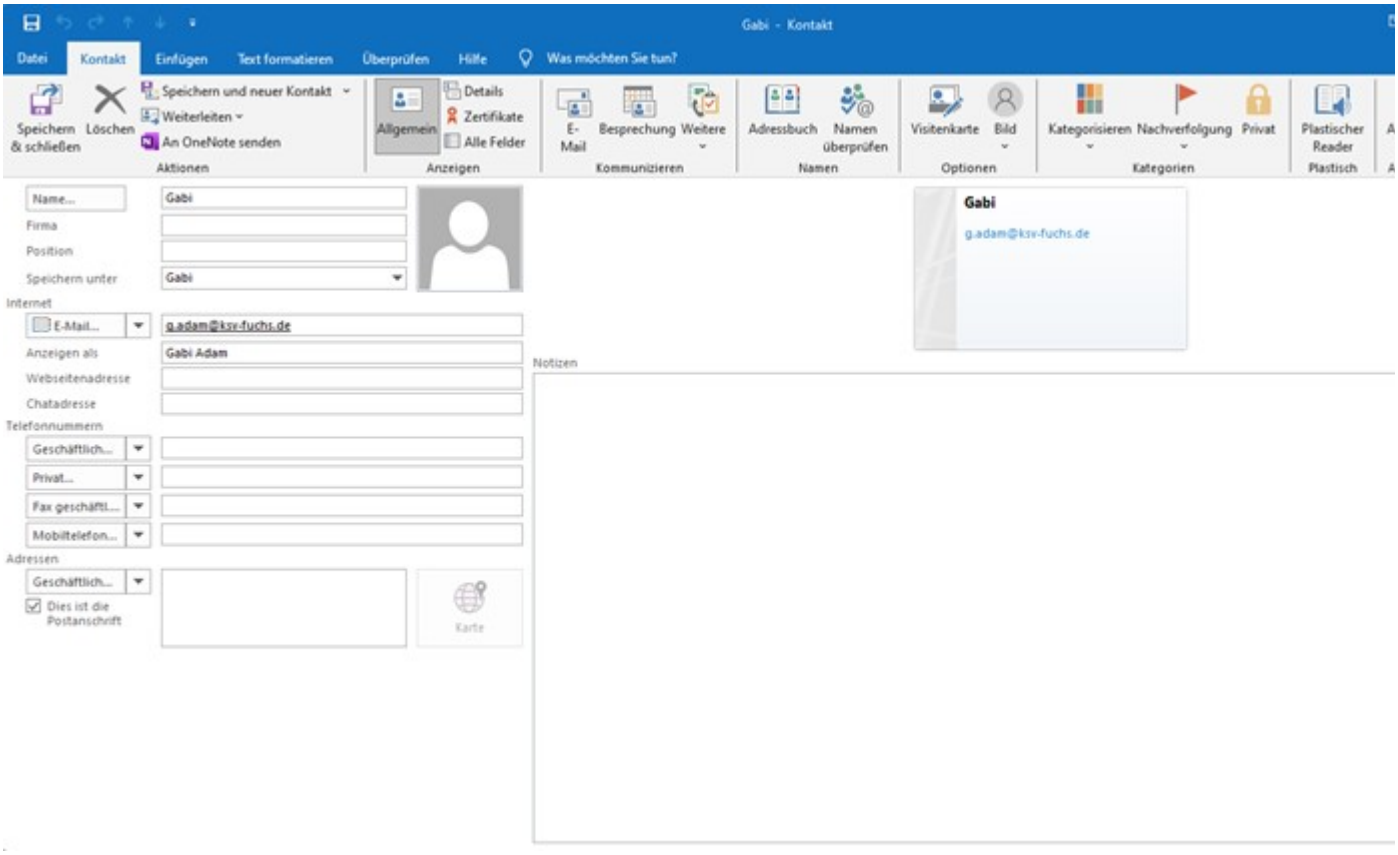
**Von:** KSV Fuchs | F. Fuchs
**Gesendet:** Mittwoch, 1. November 2023 17:10
**An:** 'NetAlive | D. Bouck-Standen'
**Cc:** 'ddehnbostel@kjkmail.de'
**Betreff:** WG: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID# 2308250050003169 / IST - Stand 31.10.2023

Bitte in auf den E-Mail-Absender schauen…
Wir können uns so nicht als „echt“ verifizieren

---

**Von:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Gesendet:** Mittwoch, 1. November 2023 17:07
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Betreff:** WG: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169 / IST - Stand 31.10.2023

Mal ganz nebenbei: So werden unsere Kontakte an Kunden, Beschwerdestellen wie z. B. Facebook versendet. Beim Empfänger kommt das dann so an:




---

**Von:** KSV Fuchs | F. Fuchs
**Gesendet:** Mittwoch, 1. November 2023 15:48
**An:** 'ddehnbostel@kjkmail.de' <ddehnbostel@kjkmail.de>
**Betreff:** WG: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169 / IST - Stand 31.10.2023

**Von:** KSV Fuchs | F. Fuchs
**Gesendet:** Mittwoch, 1. November 2023 15:47
**An:** 'Matthias Meiling (CIRT)' <Matthias.Meiling@microsoft.com>
**Cc:** 'rohn@dr-rechtsanwaelte.de' <rohn@dr-rechtsanwaelte.de>
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169 / IST - Stand 31.10.2023

**Hallo Herr Meiling,**

vielen Dank für die ausführliche Information. Zu den Cloudabhängigkeiten ist mir nur die Verbindung zu Microsoft bekannt.
Wenn ich das jetzt richtig verstehe,

- dann werden unsere bei Microsoft in der Vergangenheit gehosteten E-Mails (f.fuchs@ksv-fuchs.de, g.adam@ksv-fuchs.de und die info@ksv-fuchs.de nur weitergeleitet. Die Mails selbst können offensichtlich immer noch weiter von der „großen Unbekannten“, weiterverwendet werden?
- die Mail-Adressen müssen alle auf lokale Konten umgestellt werden, damit meinen Sie die f.fuchs@ksv-fuchs.de, die g.adam@ksv-fuchs.de und die info@ksv-fuchs.de ?
- dann eine neue Domain (musterhaft 123456789@omicrosoft.com anlegen
- einen neuen globalen Administrator für diese neue onmicrosoft.com festlegen
- … und den die „Identitätsräuber“ entfernen

Kurz gefasst habe ich versucht, die Abläufe für mich (als Nicht-IT-ler) nachzuvollziehen.

Hier müssen wir fürs erste Mal damit klarkommen. Es ist kein besonders schönes Gefühl, wenn man geklont wird und selbst keinen Einfluss mehr darauf hat, was im Internet mit den Daten passiert.

Trotzdem, vielen Dank für Ihre Bemühungen und Ihre zeitnahen Antworten auf unser seit Monaten bestehendes Problem.

**Mit freundlichen Grüßen**
**Frank Fuchs**

---

**Von:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Gesendet:** Mittwoch, 1. November 2023 13:44
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Cc:** NetAlive | D. Bouck-Standen <dbs@netalive.global>; rohn@dr-rechtsanwaelte.de
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169 / IST - Stand 31.10.2023

Hallo Herr Fuchs,

vielen Dank für Ihre E-Mail.

Da es ihr Ziel ist, sich vom dem Azure-Tenant zu trennen, würde ich folgendes empfehlen (sofern noch nicht erfolgt):

Bitte beachten Sie, dass wir als Microsoft etwaige Abhängigkeiten der Dienste zu von Ihnen verwendeten Diensten / Softwarekomponenten (Azure, andere Cloud- bzw. Online-Dienste, On-Premises etc.) nicht kennen. Bei den Empfehlungen gehe ich davon aus, dass es keinerlei Abhängigkeiten gibt. Eine entsprechende Prüfung muss Ihrerseits erfolgen. Die Ausführung der meisten Aktionen ist irreversible und sollte daher erst nach gründlicher Prüfung erfolgen.

- Umstellung Ihrer Windows Konten auf lokale Konten
- Trennung der Systeme vom Entra ID (AAD)

- Deaktivierung aller Geräte im Entra ID Portal (im späteren Verlauf können diese auch gelöscht werden, sofern durch die Deaktivierung keine Probleme entstehen). Deaktivierte Geräte können, falls Probleme auftreten, wieder reaktiviert werden.
- Erstellung einer neuen onmicrosoft.com Domain mit einer zufälligen Zeichenfolge. Diese kann einfach unter “Custom domain names” im Entra ID Portal hinzugefügt werden. Diese als primäre / initiale Domain auswählen.
- Erstellung eines neuen global Administrator Kontos unter Verwendung der neuen onmicrosoft.com Domain.
- Löschung aller Ressourcen (Benutzer, Gruppen, andere Ressourcen) welche Coldbull* oder ksv-fuch.de verwenden. Diese werden Ihnen angezeigt, wenn Sie auf die jeweilige Domain klicken.
- Entfernung der ksv-fuchs.de domain aus dem Entra ID. Ich sehe zwar auch die Option dies für die onmicrosoft.com Domain ebenfalls durchzuführen, mein Test schlug jedoch fehl. Es ist gut möglich, das diese nicht direkt entfernt werden kann.

Im Anschluss kann der Tenant stillgelegt werden. Alle hierfür notwendigen Schritte werden im folgenden Dokument beschrieben: Löschen eines Microsoft Entra-Mandanten | Microsoft Learn

Bitte lassen sie mich wissen, falls sie weitere Fragen zu dieser Thematik haben.
Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



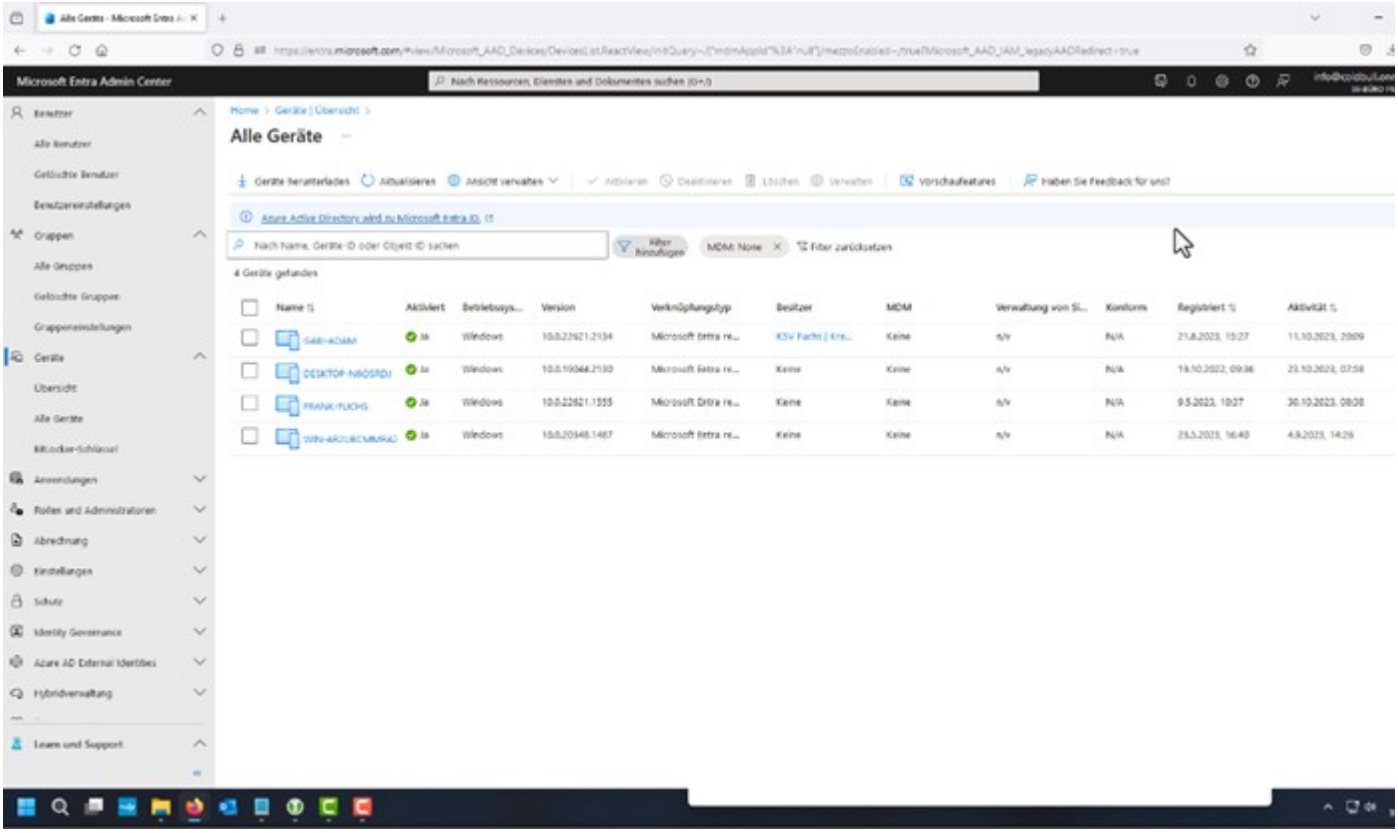
---

**Von:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Gesendet:** Wednesday, 1 November 2023 12:11
**An:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Cc:** NetAlive | D. Bouck-Standen <dbs@netalive.global>; rohn@dr-rechtsanwaelte.de
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169 / IST - Stand 31.10.2023
**Priorität:** Hoch

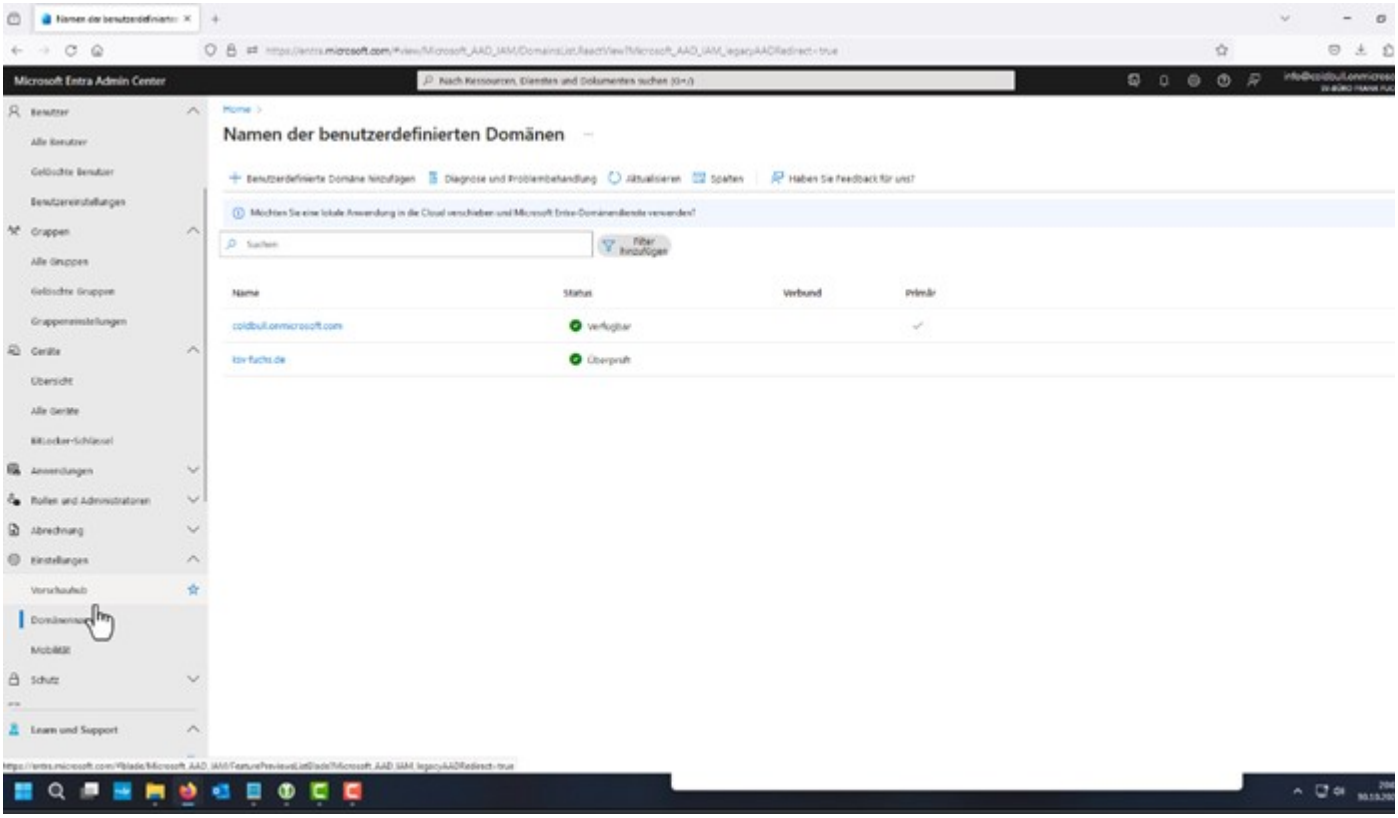
**Hallo Herr Meiling,**

nach unserer Sichtung (die technisch gesehen keine Relevanz hat!) sind dem Account folgende, für mich nicht nachvollziehbare Daten zu entnehmen:

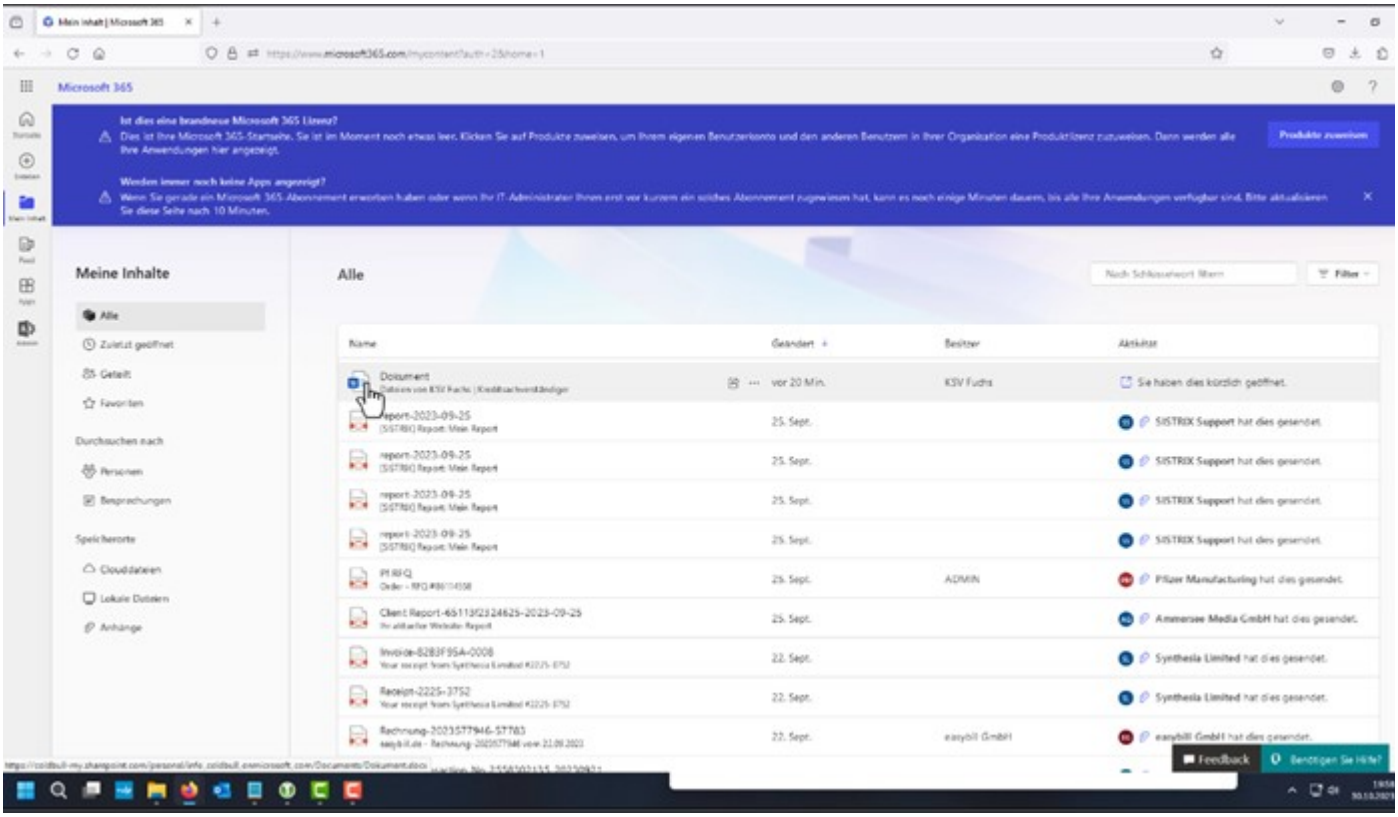
**4 Geräte zeigen den Status Aktiv an (s. Screenshot)**




Bei den benutzerdefinierten Domänen werden coldbull.onmicrosoft.com und ksv-fuchs.de angezeigt (auch wieder mit grünem Haken)




In dem Account kann man ebenfalls erkennen, dass ein Datenaustauch mit unseren Daten erfolgt ist.




Ich habe noch ein paar weiteren Screenshots erstellt und ein 30 Minuten langes Video von dem Account gemacht, welches ich bei Bedarf über die Dropbox übermitteln kann.

**Frank Fuchs**
Kreditsachverständiger

Kontakt
Ludwig-Erhard-Allee 10
76131 Karlsruhe

Tel.: +49 (0)721 4807 4650

E-Mail: f.fuchs@ksv-fuchs.de
Website: https://ksv-fuchs.de/

USt.-ID: DE288421884

KSV FUCHS
WIR PRÜFEN IHREN KREDIT

**Mitglied beim Bundesverband Deutscher Sachverständiger und Fachgutachter e.V.**

Mitglied im Bundesverband
Deutscher Sachverständiger
und Fachgutachter e.V.

---

**Von:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Gesendet:** Dienstag, 31. Oktober 2023 15:34
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Cc:** Microsoft Support <supportmail@microsoft.com>
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs,

vielen Dank für Ihre Rückmeldung.
Dann wissen wir zumindest, warum die Anmeldungen fehlgeschlagen sind und müssen nicht den Weg über eine Tenant/Instanz-Übernahme gehen.

Bitte lassen sie mich wissen, falls sie weitere Fragen zu dieser Thematik haben.
Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**Von:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Gesendet:** Monday, 30 October 2023 18:06
**An:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Meiling,

vielen Dank für das informative Gespräch.

Wir konnten über Herr Bouckstanden herausfinden, dass es noch einen aktiven Account gibt. Hierbei handelt es sich um die E-Mail mit folgendem Namen:
info@coldbull.onmicrosoft.com

**Alle anderen Benutzer wurden entfernt.**

Herr D. Bouckstanden meinte, dass der Zugang über unsere Verifikationsapp möglich sei. Wir werden das dann am Mittwoch versuchen.
Auch das Formular für GitHub wird am Mittwoch fertig sein.

**Frank Fuchs**
Kreditsachverständiger

Kontakt
Ludwig-Erhard-Allee 10
76131 Karlsruhe

Tel.: +49 (0)721 4807 4650

E-Mail: f.fuchs@ksv-fuchs.de
Website: https://ksv-fuchs.de/

USt.-ID: DE288421884


**Mitglied beim Bundesverband Deutscher Sachverständiger und Fachgutachter e.V.**




---

**Von:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Gesendet:** Montag, 30. Oktober 2023 14:38
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs,

sicher, ich rufe Sie dann an.

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**Von:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Gesendet:** Monday, 30 October 2023 14:26
**An:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Vielen Dank!

Könnten wir den Termin übers Telefon machen? Wir haben aus Sicherheitsgründen alles andere an unseren Rechnern abgeschaltet.

**Hier ist unsere Privatnummer: 07247-9851294**

---

**Von:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Gesendet:** Montag, 30. Oktober 2023 14:13
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs,

ok, ich schicke Ihnen gleich eine Einladung für 16:30 (ich bin vorher noch beim Arzt und eigentlich krankheitsbedingt nicht verfügbar, habe jedoch aktuell keinen deutschsprachigen Kollegen, der sich der Thematik annehmen kann).

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.

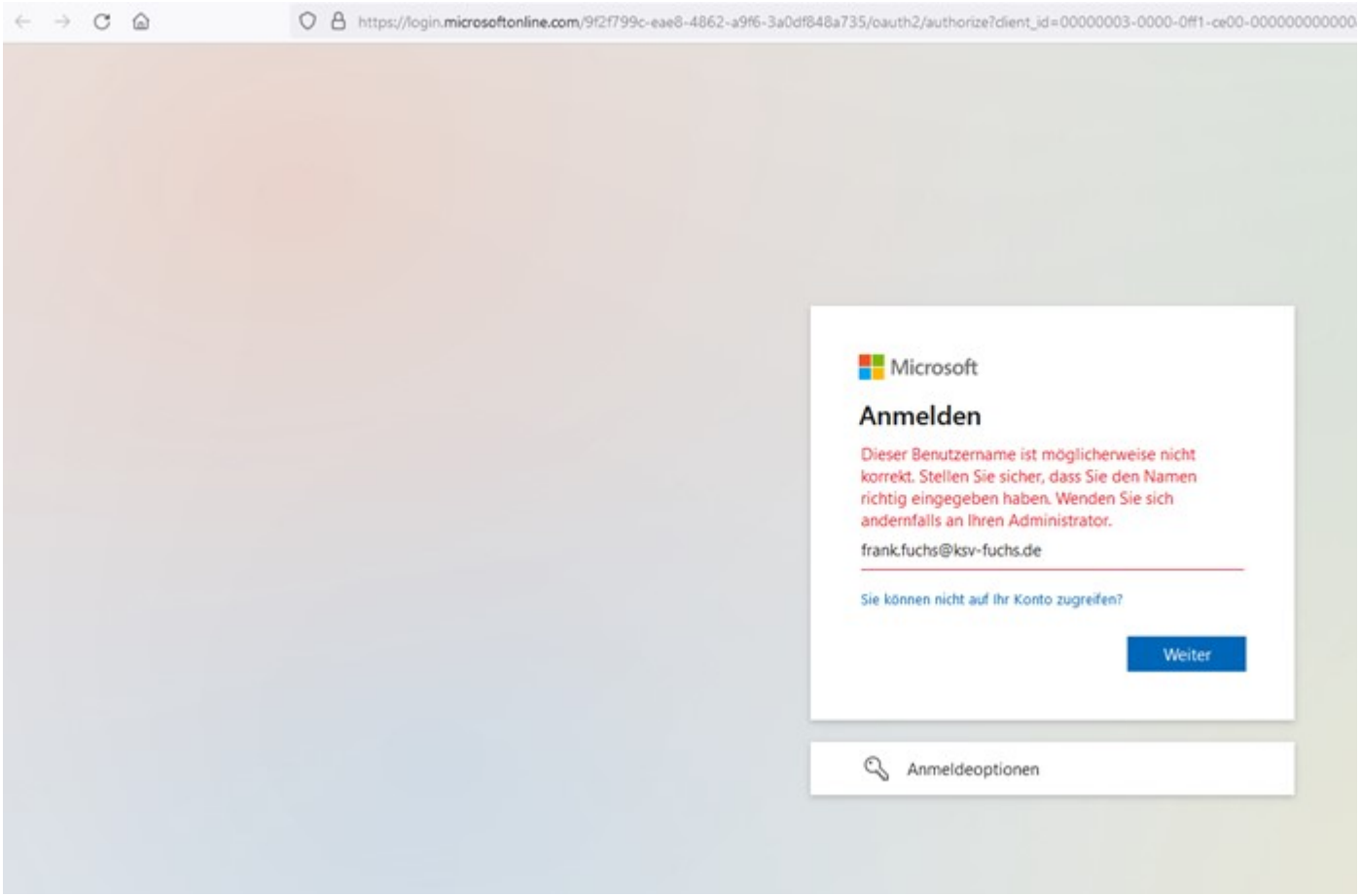
**Note:** The information contained in this message may be confidential information subject to the terms and conditions of a confidentiality agreement between Microsoft and you or your employer. You are not permitted to disclose or publish confidential information. In addition, if you have received this message in error (i) please notify us immediately by return message, and (ii) any use or distribution of this information is prohibited.
S:SF-O

---

**Von:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Gesendet:** Monday, 30 October 2023 13:51
**An:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Betreff:** WG: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

**Hallo Herr Meiling,**

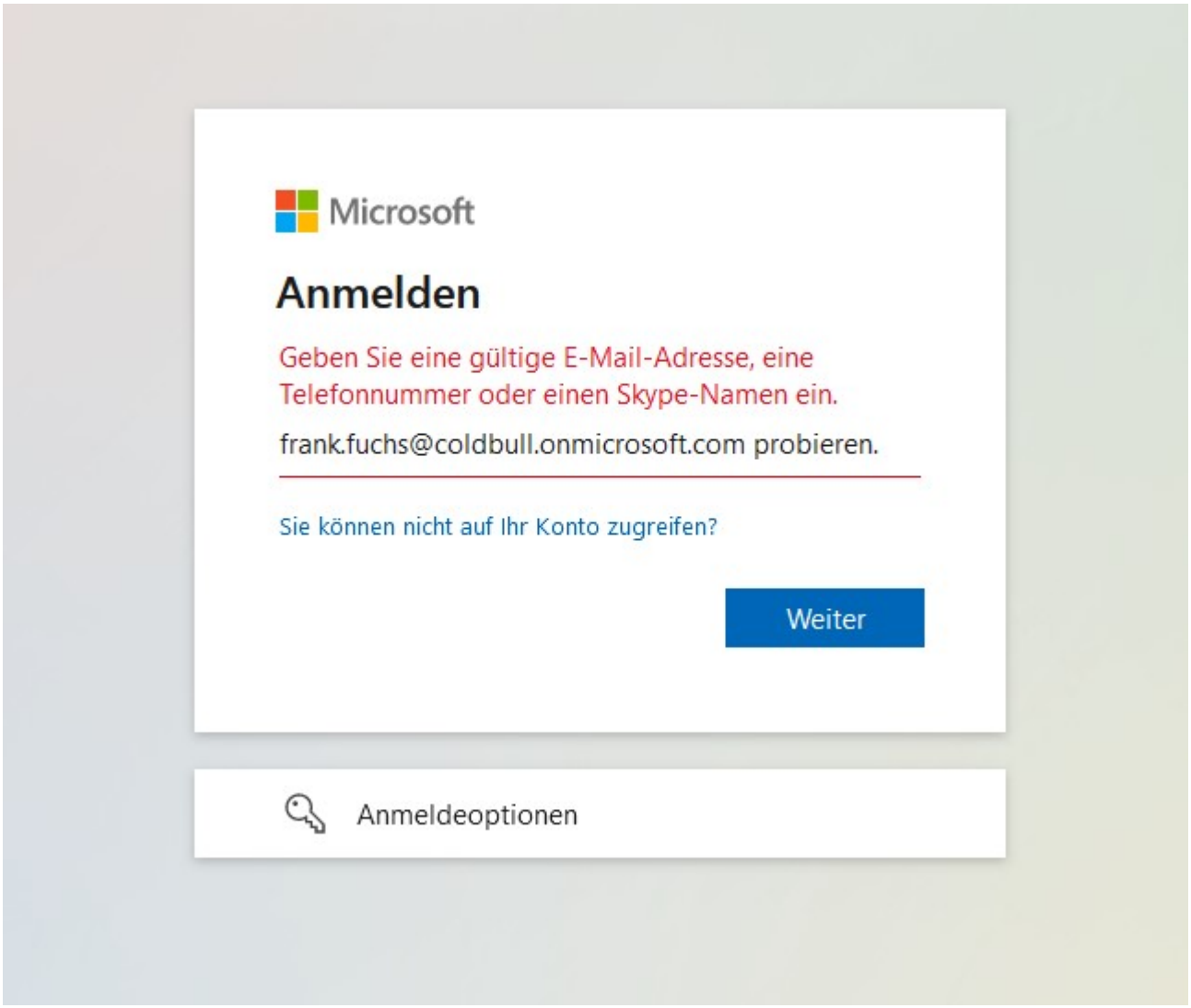
leider nicht. Bei frank.fuchs@ksv-fuchs.de und info@ksv-fuchs.de kommt diese Meldung.




Und die anderen beiden Konten kennen wir nicht: f.fuchs@coldbull.onmicrosoft.com oder frank.fuchs@coldbull.onmicrosoft.com

Bei dieser Coldbull Adresse handelt es sich ja um die Domain die von Herrn Wimmer ohne unser Wissen angelegt wurde.

Bei einem von beiden kann man sich aber offensichtlich noch mit einer Telefonnummer oder Skyp anmelden?




Wenn es ok für Sie ist, dann würden wir gerne auf Ihr Angebot zurückkommen und heute Nachmittag mit Ihnen telefonieren.

---

**Von:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Gesendet:** Montag, 30. Oktober 2023 13:33
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Cc:** rohn@dr-rechtsanwaelte.de
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs,

die SharePoint-E-Mail wurde an frank.fuchs@ksv-fuchs.de gesendet. Können Sie es hiermit einmal versuchen. Oder alternativ mit info@ksv-fuchs.de, f.fuchs@coldbull.onmicrosoft.com oder frank.fuchs@coldbull.onmicrosoft.com probieren.

Ich kann leider den aktuellen IST-Zustand Ihrer Konten nicht einsehen, da bei der Falleröffnung ausgewählt wurde, dass Sie keine Daten teilen möchten. Falls keiner der Kennungen funktioniert, und Sie über kein anderes Konto verfügen (Sie oder Ihre Kollegen), können wir nur den Weg einer Tenant Übernahme (übernähme der Azure-Instanz) einschlagen (da die Konten wahrscheinlich umbenannt oder gelöscht wurden).

Wir können gern heute Nachmittag hierzu telefonieren. Allerdings darf ich Ihnen nur generelle Empfehlungen geben und keine IT-Operationen durchführen.

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**Von:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Gesendet:** Monday, 30 October 2023 12:55
**An:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Cc:** rohn@dr-rechtsanwaelte.de; Klaus Bassler <klausba@MICROSOFT.com>
**Betreff:** WG: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

**Hier nochmal die Mail von heute Morgen.**

Herr Bouck-Standen ist aktuell im Urlaub und kann nicht weiterhelfen. Können Sie uns hier unterstützen?
Der Schaden wird für uns täglich größer !!!!!!!!!!

---

**Von:** KSV Fuchs | F. Fuchs
**Gesendet:** Montag, 30. Oktober 2023 08:42
**An:** 'Matthias Meiling (CIRT)' <Matthias.Meiling@microsoft.com>
**Cc:** 'klausba@MICROSOFT.com' <klausba@MICROSOFT.com>; 'NetAlive | D. Bouck-Standen' <dbs@netalive.global>; 'rohn@dr-rechtsanwaelte.de' <rohn@dr-rechtsanwaelte.de>
**Betreff:** WG: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

**Ergänzend möchte ich diese Mail noch an unseren Rechtsanwalt Rohn von der Kanzlei Dillerup & Rohn senden**, der die Firma GitHub inkl. Analysebericht, bereits am 18.09.2023 angeschrieben hat.
Die Folgen aus derartigen Ereignissen, sind für mich als Betroffenen kaum mehr in Worte zu fassen.
Bei der Nutzung von bezahlbaren Produkten der Firma Microsoft, habe ich mit solchen, möglichen Auswüchsen nicht gerechnet.

---

**Von:** KSV Fuchs | F. Fuchs
**Gesendet:** Montag, 30. Oktober 2023 08:24
**An:** 'Matthias Meiling (CIRT)' <Matthias.Meiling@microsoft.com>
**Cc:** 'klausba@MICROSOFT.com' <klausba@MICROSOFT.com>; 'NetAlive | D. Bouck-Standen' <dbs@netalive.global>; 'NetAlive | D. Bouck-Standen' <dbs@netalive.global>
**Betreff:** WG: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

**Guten Morgen Herr Mailing,**

inzwischen überschlagen sich bei uns die Ereignisse. Im Anhang füge ich Ihnen 2 E-Mail bei, aus denen Sie die Verbindung zwischen GitHub, Manuel Wimmer und Microsoft entnehmen können.

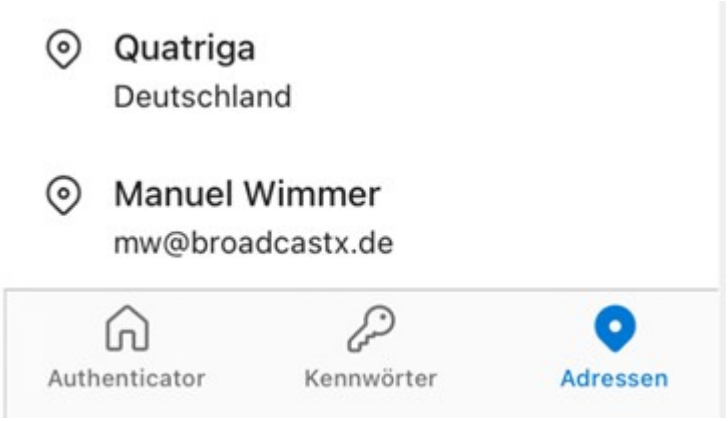
**Kurz gesagt:**

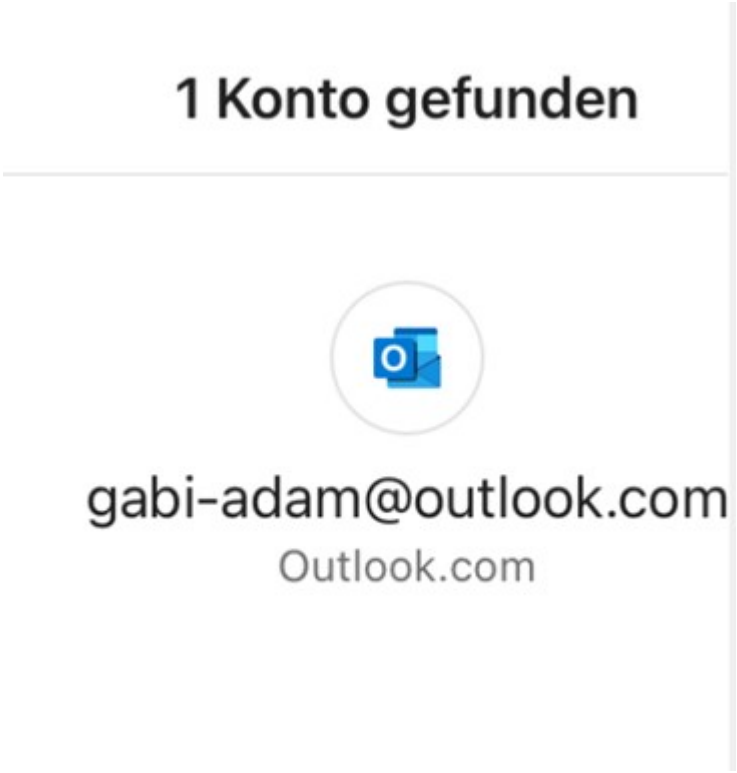
Herr Wimmer hat mit seinen Zugangsmöglichkeiten über GitHub, auch das I-Phone Handy von Frau Adam übernommen, mit welchem über den 2-Stufen Verifikationsprozess der Microsoft-App, alle Freigaben von uns erfolgten.

Betroffen sind alle Sozialen Netzwerke, inkl. Firmenwebseite und wie man sieht, auch ein neu aufgesetzter Rechner.

Auch die Vereinsseite von quatriga-21.de, bei der Frau Adam 2. Vorsitzende ist, ist betroffen.

Auszug aus der beigefügten E-Mail:




Sie erhalten auch nochmal die Mail vom 02.10.2023 von Herrn Bassler, den Beginn an bemüht war, dieses Problem zu lösen und vermutlich als Einziger, die Gefahr aus dieser Domain coldbull.onmicrosoft.com erkannt hat.

**Kopie dieser Mail an**
Klaus Bassler, Microsoft
D.Bouck-Standen, Firma Netalive

**Frank Fuchs**
Kreditsachverständiger

Kontakt
Ludwig-Erhard-Allee 10
76131 Karlsruhe

Tel.: +49 (0)721 4807 4650

E-Mail: f.fuchs@ksv-fuchs.de
Website: https://ksv-fuchs.de/

USt.-ID: DE288421884

KSV FUCHS
WIR PRÜFEN IHREN KREDIT

**Mitglied beim Bundesverband Deutscher Sachverständiger und Fachgutachter e.V.**

Mitglied im Bundesverband Deutscher Sachverständiger und Fachgutachter e.V.
BDSF

---

**Von:** KSV Fuchs | F. Fuchs
**Gesendet:** Samstag, 28. Oktober 2023 13:55
**An:** 'Matthias Meiling (CIRT)' <Matthias.Meiling@microsoft.com>
**Cc:** 'NetAlive | D. Bouck-Standen' <dbs@netalive.global>
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

**Hallo Herr Meiling,**

Herr Bouck-Standen hat gestern eine Vollmacht von mir erhalten, um mit GitHub direkt zu kommunizieren, da uns das technische Verständnis hierzu schlicht und ergreifend fehlt.

Heute ging bei uns eine E-Mail ein, die ich Ihnen als PDF beifüge. Die Mail ist von Microsoft Sharepoint, zumindest steht das im Absender. Angeklickt haben wir den Link nicht, weil wir uns nicht sicher sind, ob diese Mail nicht auch wieder ein Fake ist.

In allen sozialen Medien haben wir mittlerweile Probleme mit der Verifizierung unserer Identität.

Wir sind zudem auf eine Mail gestoßen, die lautet: f.fuchs@outlook.com. Diese Mail wurde nicht von mir angemeldet. Ich habe zwar eine private Outlook-Adresse, aber die lautet anders.

Können Sie diesem Vorgang bitte nachgehen?

Vielen Dank im Voraus

**Frank Fuchs**
Kreditsachverständiger

Kontakt
Ludwig-Erhard-Allee 10
76131 Karlsruhe

Tel.: +49 (0)721 4807 4650

E-Mail: f.fuchs@ksv-fuchs.de
Website: https://ksv-fuchs.de/

USt.-ID: DE288421884

Mitglied im Bundesverband
Deutscher Sachverständiger
und Fachgutachter e.V.



**Von:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Gesendet:** Freitag, 27. Oktober 2023 10:19
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Cc:** rohn@dr-rechtsanwaelte.de; Microsoft Support <supportmail@microsoft.com>
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs,

ich möchte mich gern nach dem aktuellen Stand erkunden.

Hatten Sie die Möglichkeit, mit Ihrem IT-Dienstleister an der Bereinigung der Azure-Instanz zu arbeiten? Haben Sie hierauf administrativen Zugriff?

Konnten Sie das GitHub-Formular ausfüllen und absenden?

Vielen Dank vorab und ein angenehmes Wochenende.

Mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



**Von:** Matthias Meiling (CIRT)
**Gesendet:** Tuesday, 24 October 2023 11:42
**An:** 'KSV Fuchs | F. Fuchs' <frank.fuchs@ksv-fuchs.de>

**Cc:** rohn@dr-rechtsanwaelte.de
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs,

vielen Dank für Ihre Nachricht.

Mit Bezug auf Azure:

Wie im Telefonat besprochen, haben wir keine Möglichkeit, Ressourcen aus ihrer Azure Umgebung (Tenant) zu entfernen.

Sofern Sie, respektive ihr Dienstleister Zugriff auf die Umgebung hat (was der Fall zu sein scheint, da Sie hierüber auch die Support-Anfrage eröffnet hatten), und über Administrator-Berechtigungen verfügen, können Sie etwaige Konten löschen und Passwörter zurücksetzen, um Dritte auszusperren. Weiterhin haben Sie die Möglichkeit, Ressourcen zu löschen. Herr Bouck-Standen wollte Sie, wie telefonisch vereinbart, dabei unterstützen,

Falls Sie über keinen Zugang mit Administrator-Berechtigungen verfügen, habe ich die Möglichkeit, über unser Azure Subscription Management Support Team einen entsprechenden Prozess anzustoßen, um Ihnen den Zugang zu ermöglichen.

Ich habe soeben nochmals geschaut, ob ich Hinweise darauf finde, das neue Ressourcen innerhalb Ihrer Umgebung ausgerollt wurden. Dies scheint nicht der Fall zu sein.
Andere Änderungen kann ich leider nicht einsehen (diese sollten jedoch im Azure Audit log für Sie / Ihren Dienstleister einsehbar sein – zumindest für die letzten 7 Tage).

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**Von:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Gesendet:** Monday, 23 October 2023 18:37
**An:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Cc:** rohn@dr-rechtsanwaelte.de
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

**Hallo Herr Meiling,**

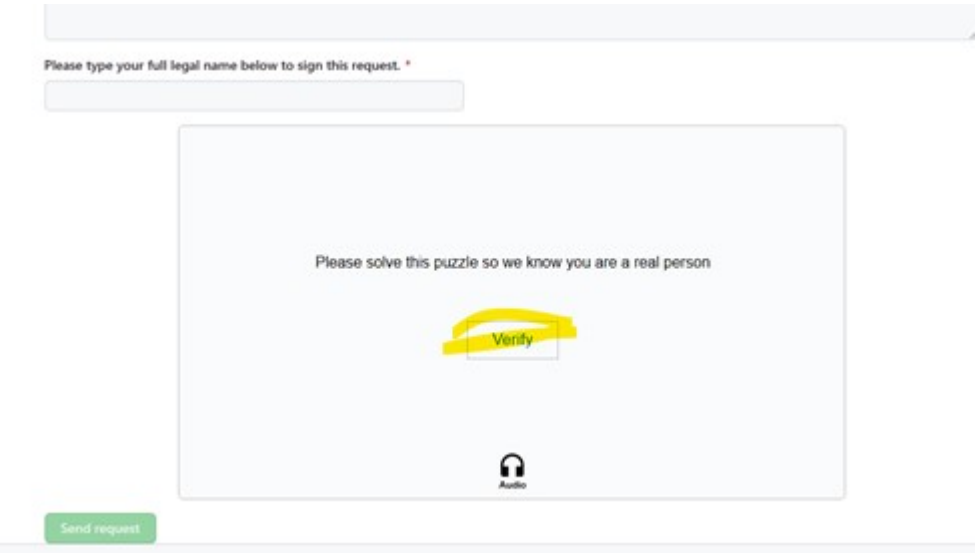
unabhängig von GitHub, tut Microsoft ja auch nichts. Herr Wimmer ist immer noch mit der Coldbull-Domain unterwegs und verrichtet tagtäglich neue Schäden.
Es hindert ihn ja auch niemand daran!

Wir werden morgen nochmals versuchen dieses Formular auszufüllen.

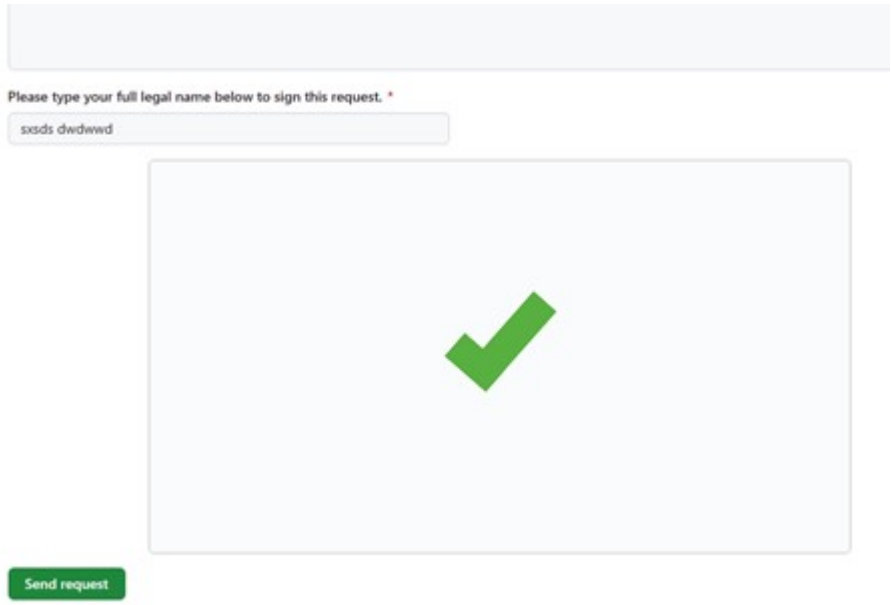
**Von:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Gesendet:** Montag, 23. Oktober 2023 17:31
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Cc:** dialogue@netalive.it
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs,

Ich habe mir das Formular angeschaut – eine Anmeldung scheint nicht notwendig zu sein (ich bin ebenfalls nicht angemeldet).
Ich musste jedoch hierzu erfolgreich die Anti-Spam Verifizierung durchführen:




Im Anschluss wäre ich in der Lage gewesen, das Formular abzusenden.




Haben Sie diesen Schritt ebenfalls durchgeführt? Aus dem PDF wird dies leider nicht deutlich. Alle anderen Pflichtfelder scheinen ausgefüllt zu sein.

Wie bereits erwähnt, handelt es sich bei GitHub nicht um Microsoft, sondern um eine eigenständige Firma. Daher kann ich Ihnen hierbei auch nur aus Sicht eines “außenstehenden” behilflich sein.

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**Von:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Gesendet:** Monday, 23 October 2023 17:05
**An:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Cc:** dialogue@netalive.it
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

**Hallo Herr Meiling,**

ich füge Ihnen im Anhang ein ausgefülltes Formular aus meiner Sicht bei. Wie Sie dieser PDF-Datei entnehmen können, funktioniert eine Übertragung an GitHub nicht. Offensichtlich muss man dafür eingeloggt sein?
Herr Bouck-Standen ist aktuell zeitlich sehr eingespannt, weshalb er noch keine Zeit gefunden hat, sich mit diesem Formular zu beschäftigen.

GitHub liegt zudem eine ausführliche Analyse zu dem besagten Konto vor, genauso wie Microsoft seit Monaten die Brisanz kennt.

Sollte das auf diesem Weg nicht funktionieren, dann müssen wir zur gegebenen Zeit andere Wege suchen, um diesem unheilbaren Zustand entgegen zu wirken.

**Frank Fuchs**
Kreditsachverständiger

Kontakt
Ludwig-Erhard-Allee 10
76131 Karlsruhe

Tel.: +49 (0)721 4807 4650

E-Mail: f.fuchs@ksv-fuchs.de
Website: https://ksv-fuchs.de/

USt.-ID: DE288421884

KSV FUCHS
WIR PRÜFEN IHREN KREDIT

**Mitglied beim Bundesverband Deutscher Sachverständiger und Fachgutachter e.V.**




---

**Von:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Gesendet:** Montag, 23. Oktober 2023 15:14
**An:** dialogue@netalive.it
**Cc:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>; Microsoft Support <supportmail@microsoft.com>
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Bouck-Standen, hallo Herr Fuchs,

ich möchte mich gerne nach dem aktuellen Stand erkundigen:
- Wurde die Anfrage bei GitHub eröffnet?
- Haben Sie sonst noch Fragen zu Thema Azure hierzu?

Falls Sie keine Fragen zum Thema Azure Security haben, würde ich vorschlagen, dass ich diese Anfrage archiviere (Sie können mir selbstverständlich im Nachgang weiterhin die GitHub-Bearbeitungsnummer nennen, die ich dann gerne an die Kollegen von GitHub-SecOps weiterleite).

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**Von:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Gesendet:** Tuesday, 17 October 2023 12:08
**An:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>

**Cc:** dialogue@netalive.it
**Betreff:** WG: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

**Hallo Herr Meiling,**

Herr Bouckstanden wird das Formular in technischer Hinsicht zeitnah beantworten. Bitte entschuldigen Sie die Zeitverzögerung.

**Mit freundlichen Grüßen**
**Frank Fuchs**

---

**Von:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Gesendet:** Dienstag, 17. Oktober 2023 11:09
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Cc:** rohn@dr-rechtsanwaelte.de; dialogue@netalive.it; Microsoft Support <supportmail@microsoft.com>
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs,

ich möchte mich gerne nach dem aktuellen Stand erkundigen:
Hatten Sie bei GitHub das Formular ausgefüllt?
Gibt es sonst noch Fragen bzgl. dieser Anfrage (Thema Azure)?

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**Von:** Matthias Meiling (CIRT)
**Gesendet:** Thursday, 12 October 2023 11:48
**An:** 'KSV Fuchs | F. Fuchs' <frank.fuchs@ksv-fuchs.de>
**Cc:** rohn@dr-rechtsanwaelte.de; dialogue@netalive.it; dialogue@netalive.it
**Betreff:** RE: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs,

vielen Dank für Ihre E-Mail.

Um die Thematik zu adressieren, muss das Abuse-Formular (Missbrauch der Platform) verwendet werden, um dies gegenüber GitHub anzuzeigen. Eine E-Mail stellt keine Bearbeitung sicher.
Die Meldung kann nur durch Sie oder Ihre rechtliche Vertretung erfolgen, nicht jedoch von Dritten (wie mir).

Das Formular kann sowohl für die Anforderung zur Abschaltung als auch Übernahme der betroffenen GitHub-Instanz verwendet werden. Dies sollte entsprechend mit angegeben werden.

Ich schlage vor, dass wir den Prozess von GitHub folgen, um eine zeitnahe Bearbeitung zu gewährleisten. Alles andere führt entweder zu Verzögerungen oder verläuft erfolglos.

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**From:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Sent:** Wednesday, 11 October 2023 18:34
**To:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Cc:** rohn@dr-rechtsanwaelte.de; dialogue@netalive.it; dialogue@netalive.it
**Subject:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169
**Importance:** High

**Hallo Herr Meiling,**

von Rechtsanwalt Rohn wurde bereits eine Erläuterung an GitHub mit einem entsprechenden Bericht übermittelt. Dieses Formular ist insoweit für mich unverständlich, da aus dem Anschreiben von Rechtsanwalt Rohn nebst Anlage bereits alles erläutert wurde.
Unter diesem Link finden Sie das Produkt, welches nach unseren Vorgaben von der Firma Herrn Manuel Wimmer, Geschäftsführer der Firma BroadcastX (Link: Ihre IT Agentur in Hutthurm bei Passau | BroadcastX GmbH) erstellt wurde.
ZINS ID Starter für Steuerberater und Steuerbüros (ksv-fuchs.de)

Hierbei wurden unsere Geschäftsgeheimnisse von Herrn Wimmer verarbeitet. Alle weiterführenden Informationen, sind der Analyse von Herrn Dawid Bouckstanden zu entnehmen.

**Mit freundlichen Grüßen**

Frank Fuchs

---

**Von:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Gesendet:** Mittwoch, 11. Oktober 2023 17:19
**An:** RA Rohn - Dillerup & Rohn Rechtsanwälte <rohn@dr-rechtsanwaelte.de>; KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Betreff:** RE: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Rohn, hallo Herr Fuchs,

die Kollegen vom Sicherheits-Team bei GitHub haben sich nochmals gemeldet und gebeten, dass das folgende Formular ausgefüllt wird: https://support.github.com/contact/dmca-takedown.

Im Anschluss erhalten Sie eine Bearbeitungsnummer. Bitte teilen Sie mir diese mit, ich leite diese dann wiederum an die Kollegen weiter.

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**From:** Matthias Meiling (CIRT)
**Sent:** Tuesday, 10 October 2023 14:32
**To:** 'RA Rohn - Dillerup & Rohn Rechtsanwälte' <rohn@dr-rechtsanwaelte.de>; 'frank.fuchs@ksv-fuchs.de' <frank.fuchs@ksv-fuchs.de>
**Subject:** RE: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Rohn, hallo Herr Fuchs,

Ich habe bereits Rückmeldung von GitHub's Sicherheits-Team bekommen. Die Kollegen werden dies mit Priorität an den GitHub Support weitergeben und sich bei Ihnen melden.

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.

**Note:** The information contained in this message may be confidential information subject to the terms and conditions of a confidentiality agreement between Microsoft and you or your employer. You are not permitted to disclose or publish confidential information. In addition, if you have received this message in error (i) please notify us immediately by return message, and (ii) any use or distribution of this information is prohibited.
S:SF-O

---

**From:** Matthias Meiling (CIRT)
**Sent:** Tuesday, 10 October 2023 11:52
**To:** 'RA Rohn - Dillerup & Rohn Rechtsanwälte' <rohn@dr-rechtsanwaelte.de>

**Cc:** frank.fuchs@ksv-fuchs.de
**Subject:** RE: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Rohn, hallo Herr Fuchs,

vielen Dank für die schnelle Rückmeldung.

Ich werde mit den bereitgestellten Informationen versuchen, an GitHub heranzutreten, um weitere Informationen zu erhalten.
Bei GitHub Inc. handelt es sich um eine eigenständige Firma, weshalb ich nicht einschätzen kann, ob und in welcher Form ich eine Rückmeldung erhalten werde.

ich halte Sie hierzu auf dem Laufenden.

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**From:** RA Rohn - Dillerup & Rohn Rechtsanwälte <rohn@dr-rechtsanwaelte.de>
**Sent:** Tuesday, 10 October 2023 11:32
**To:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Cc:** frank.fuchs@ksv-fuchs.de
**Subject:** WG: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169
**Importance:** High

> You don't often get email from rohn@dr-rechtsanwaelte.de. Learn why this is important

Sehr geehrter Herr Meiling,

in der vorbezeichneten Angelegenheit kommen wir auf den Vorgang zurück und nehmen auf Ihre untenstehende E-Mail Bezug, die uns von unserer Mandantschaft weitergeleitet wurde. Bitte entschuldigen Sie die aufgrund einer hohen Arbeitsauslastung ungewöhnlich lange Bearbeitungszeit.

Anbei erhalten Sie unser Anschreiben an die Github Inc, die wir am 18. September 2023 an mehrere E-Mail-Adressen des Unternehmens versandt hatten. Eine Rückmeldung steht nach wie vor aus.

Sollten Sie weitere Rückfragen haben oder Informationen benötigen, stehen wir gerne zur Verfügung.

Damit verbleibe ich für heute
mit freundlichen Grüßen

Lars Rohn (Rechtsanwalt)

_____
Dillerup & Rohn Rechtsanwälte PartGmbB
Moltkestr. 19
48151 Münster
Telefon: +49 251 13 46 76 60
Telefax: +49 251 13 46 76 70
E-Mail: rohn@dr-rechtsanwaelte.de
Internet: www.dr-rechtsanwaelte.de
**KANZLEI FÜR BANKRECHT & ANLEGERSCHUTZ**

**Sitz der Partnerschaftsgesellschaft mbB**
**Münster**
**AG Essen | PR 3905**
**USt-ID: DE310626552**

**DR Rechtsanwälte - MIT KOMPETENZ & LEIDENSCHAFT**

---

**Von:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Gesendet:** Dienstag, 10. Oktober 2023 10:30
**An:** Matthias Meiling (CIRT) <Matthias.Meiling@microsoft.com>
**Cc:** RA Rohn - Dillerup & Rohn Rechtsanwälte <rohn@dr-rechtsanwaelte.de>; dialogue@netalive.it
**Betreff:** AW: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169
**Priorität:** Hoch

Hallo Herr Meiling,

unser Rechtsanwalt wird Ihnen die Unterlagen von Github zukommen lassen.
Wenn Sie diese Unterlagen haben, können wir gerne nochmal telefonieren.

Mit freundlichen Grüßen
Frank Fuchs

---

**Von:** Matthias Meiling (CIRT) < >
**Gesendet:** Dienstag, 10. Oktober 2023 10:26
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>; dialogue@netalive.it
**Cc:** Microsoft Support <supportmail@microsoft.com>
**Betreff:** RE: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs, hallo Herr Bouck-Standen,

hiermit möchte ich mich gern nach dem aktuellen Stand der Bereinigungsarbeiten erkundigen.
Gibt es hierzu von Ihrer Seite noch Fragen? Anderenfalls würde ich diese Anfrage archivieren.

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**From:** Matthias Meiling (CIRT)
**Sent:** Thursday, 5 October 2023 15:39
**To:** 'frank.fuchs@ksv-fuchs.de' <frank.fuchs@ksv-fuchs.de>
**Cc:** Microsoft Support <supportmail@microsoft.com>; 'dialogue@netalive.it' <dialogue@netalive.it>
**Subject:** RE: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs,

bzgl. der GitHub-Thematik – möchten Sie, das ich intern versuche, an das GitHub-Security Team heranzutreten, um zu prüfen, welche Möglichkeiten es gibt, ihre GitHub-Präsenz (Repository) zu entfernen? Falls das der Fall ist, bitte ich Sie, mir Ihre bestehende Korrespondenz mit dem GitHub-Support (inkl. Referenznummer etc.) und den Link zu “ihrer” GitHub-Seite zu übermitteln.

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.

**Note:** The information contained in this message may be confidential information subject to the terms and conditions of a confidentiality agreement between Microsoft and you or your employer. You are not permitted to disclose or publish confidential information. In addition, if you have received this message in error (i) please notify us immediately by return message, and (ii) any use or distribution of this information is prohibited.
S:SF-O

---

**From:** Matthias Meiling (CIRT)
**Sent:** Wednesday, 4 October 2023 16:27
**To:** frank.fuchs@ksv-fuchs.de; dialogue@netalive.it
**Cc:** Microsoft Support <supportmail@microsoft.com>
**Subject:** RE: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuchs, hallo Herr Bouck-Standen,

vielen Dank nochmals für die Teilnahme an der Telefonkonferenz.

Bzgl. Github konnte ich leider nur die folgende Seite finden: Reporting abuse or spam - GitHub Docs.

Sofern ich mich erinnern kann, wurde erwähnt, dass Sie bereits versucht haben, mit dem GitHub-Support in Kontakt zu treten.
Können Sie mir hierzu ggf. die Korrespondenz weiterleiten? Bitte senden Sie mir auch den Link zur betroffenen GitHub-Seite. Ich würde dann prüfen, ob ich intern weitere Möglichkeiten habe, Ihnen bei dieser Thematik weiterzuhelfen.

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter,
Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---

**From:** Matthias M <support@mail.support.microsoft.com>
**Sent:** Monday, 2 October 2023 14:26
**To:** frank.fuchs@ksv-fuchs.de; Microsoft Support <supportmail@microsoft.com>
**Cc:** dialogue@netalive.it
**Subject:** RE: AW: WG: [EXTERNAL] AW: Azure Konto wurde ni... - TrackingID#2308250050003169

Hallo Herr Fuch,

vielen Dank für Ihre E-Mail.

Sehr gern. Da ich heute schon ausgebucht bin und morgen Feiertag ist, würde ich den Termin für Mittwoch um 14:30 ansetzen. Falls dies zeitlich nicht passen sollte, können wir den Termin anpassen.

Ich sende Ihnen hierzu die Teams-Einladung.

Vielen Dank und mit freundlichen Grüßen,
Matthias Meiling

PS: Please always use “Reply All” to ensure proper follow-up.

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München
Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter,
Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438
Microsoft Privacy Statement – Microsoft privacy

If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---------- Original Message ----------
**From:** frank.fuchs@ksv-fuchs.de;
**Received:** Mon Oct 02 2023 14:08:13 GMT+0200 (Central European Summer Time)
**To:** supportmail@microsoft.com;
**Cc:** dialogue@netalive.it;

**Subject:** AW: WG: [EXTERNAL] AW: Azure Konto wurde nicht ... - TrackingID#2308250050003169

**Sehr geehrter Herr Meiling,**

vielen Dank für Ihre Nachricht. Gerne würden wir uns mit Ihnen über den Ablauf unterhalten, allerdings in Verbindung mit unserem neuen IT-Administrator, Herrn David Bouck-Standen. Der Einfachheit halber würden wir eine Kommunikation über MS-Teams vorschlagen. Hierzu müssten Sie uns an 2 E-Mail-Adressen eine Einladung senden:

f.fuchs@ksv-fuchs.de
dialogue@netalive.it

Unsere Verfügbarkeit wäre die ganze Woche (Ausnahme: Donnerstag!) gegeben.

Über eine Rückmeldung Ihrerseits bedanke ich mich bereits im Voraus

**Mit freundlichen Grüßen**
**Frank Fuchs**

**Von:** Matthias M <support@mail.support.microsoft.com>
**Gesendet:** Montag, 2. Oktober 2023 12:50
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>; supportmail@microsoft.com
**Betreff:** RE: WG: [EXTERNAL] AW: Azure Konto wurde nicht ... - TrackingID#2308250050003169

Sehr geehrter Herr Fuchs,

mein Name ist Matthias Meiling, ich bin vom Cybersecurity Incident Response Team (MS-CIRT) bei Microsoft. Der Kollege Baßler hat uns involviert.

Mein Team führt sog. Incident Response Analysen durch, um nach einem Angriff zu evaluieren, wie die Angreifer vorgegangen sind und welche Aktionen durchgeführt wurden (basierend auf vorhandene Datenprotokolle/Logs). Die hierzu notwendigen Logs, insb. die Entra ID Audit Logs, werden abhängig von Ihrer Entra ID (Azure AAD) Lizenz für 7 oder 30 Tage vorgehalten und im Anschluss unwiderruflich überschrieben, sofern diese nicht von Ihnen exportiert oder in einen anderen Speicherplatz übertragen werden. Sie finden weitere Informationen hierzu im unteren Bereich dieser E-Mail.

Unabhängig hiervon werden sog. Root-Cause-Analysieren seitens Microsoft nur für Kunden durchgeführt, welche über einen Microsoft Premier oder Unified Support-Vertrag verfügen. Falls ein etwaiger Vertrag nicht vorliegt, kann eine Analyse durch Sie selbst (die Kollegen von Entra ID-Team können bei Fragen zu den Logs helfen), oder durch eine von Ihnen beauftrage auf Incident Response spezialisierte Firma erfolgen. Hierzu ist es jedoch erforderlich, wie bereits ausgeführt, das entsprechende Protokoll-Informationen noch vorhanden sind. Ist dies nicht der Fall, ist eine Analyse nicht möglich.

Gern können wir hierzu auch nochmals telefonieren.
Bitte teilen Sie mir hierzu Ihre Verfügbarkeit mit.

Unabhängig hiervon senden ich Ihnen nachfolgend weitergehende Informationen, Handlungsmaßnahmen als auch Optionen für die Weiterbearbeitung dieser Anfrage. Da unser Team Anfragen ausschließlich in englischer Sprache bearbeitet, sind diese in Englisch verfasst. Falls dies ein Problem darstellt, können wir diese auch gern telefonisch durchgehen.

```
Unfortunately, this service request has been opened using a Professional Service Level
Agreement which doesn't include Incident Response Investigative Services.

You can find information on what’s included with Professional Support plans at the following
```

site: https://support.microsoft.com/en-us/help/4457997/microsoft-professional-support-pay-per-incident-faq
Incident Response Investigative Services is only provided for Unified and Premier Service Level Agreements (at the exception of ASfP - Advanced Support for Partners).

If your organization has a Unified or Premier contract, please close this case, and open a new one using one of these contracts.

If you don't have the possibility to open a request using a Unified or Premier contract, depending on your final expectations, we may be able to involve a different team to assist you:

1- If you want to raise a billing dispute for a potential high cost generated during the issue, we can move this service request to our Azure Billing team. Your request will follow a specific process to settle the dispute.
If required by the Azure Billing team, further investigations will be conducted to determine, based on the available data, what happened, how it happened, and when it happened.
Please note it is not guaranteed the investigation will be conducted as it will only be initiated based on the Azure Billing team request, if and only if it is required.

2- If you don't have any billing concerns and you have specific questions related to AAD Sign-in and Audit logs or AAD features, we can move this service request to our Azure Active Directory Support Team (AAD team).
To do so, we would need a list of questions to relay to the AAD team. If any, could you please share them with me?

3- If your request doesn't fall under one of the two options mentioned above and you're looking for an Incident Response investigation, I invite you to contact your internal security team or a vendor that would be in a position to provide this service. In this scenario, the service request will be closed.

Could you please let me know what option you would like to go with so I can act accordingly?

!!! Important information !!! Depending on the Azure Active Directory license, data history (Sign-in and Audit logs) is limited to 7 or 30 days:
- https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-data-retention
If the issue you're reporting is no longer covered in the AAD Sign-in and Audit logs, it won't be possible for anyone to provide any additional information as the data no longer exist.
If you still have access to the data, we encourage you to archive them before reaching the data history limit, else they will be gone, for you and for Microsoft:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-logs-and-reporting

In the eventuality you would like to investigate the issue yourself, you should be able to find relevant information in the following logs:
- AAD Sign-in logs: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-all-sign-ins
- AAD Audit logs: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs
- Activity logs: https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log?tabs=powershell

You should also review:
- The created resources for any unexpected/malicious entries. In the Azure Portal, select your subscription and under "Settings" open "Resources"
- The AAD registered applications for any unexpected/malicious entries. In the Azure Portal, select "Azure Active Directory" and under "Manage" open "App registrations". Then click on "View all applications in the directory"
- The recently created accounts (internal and guest) and their permissions and roles on AAD and on the subscription

For any account identified as performing non-legitimate or suspicious activities, start with the following steps:

- Perform a password reset
- Block the account if you suspect the attacker can reset the password or do multi-factor authentication in place of the legitimate user
- Review the permissions and roles assigned to the account on AAD and on the subscription
- Revoke refresh tokens: https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/users-revoke-access
- Disable any managed devices considered compromised: https://learn.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal
- Delete any resources / applications maliciously created by the account

To go further, don't hesitate to review and apply https://learn.microsoft.com/en-us/azure/security/fundamentals/recover-from-identity-compromise#identify-indications-of-compromise

If you're using Defender for Cloud Apps, leverage this article to hunt for compromised Azure subscriptions:
https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/hunt-for-compromised-azure-subscriptions-using-microsoft/ba-p/3607121

To improve the security posture and reduce the risk of a new security incident, we strongly recommend following this article: https://www.microsoft.com/security/blog/2020/07/15/prevent-identity-attacks-azure-active-directory/
The first critical step to perform, if not already done, is to enable MFA as part of your security foundation.
Start with each of your privileged accounts, whether they are part of this incident or not, and then extend it to everyone.
MFA is indeed a low configuration effort leading to high impact on the overall security posture.

It is also recommended to not only authenticate the user but also the device. It will prevent any bad actor to connect to resources from a non-authorized device with a stolen token.
More information available here: https://docs.microsoft.com/en-us/mem/intune/protect/create-conditional-access-intune

Additionally, you may consider the new Token Protection for Sign-In Sessions approach:
https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/public-preview-token-protection-for-sign-in-sessions/ba-p/3815756

Another important action is to leverage security solutions that will monitor, alert and/or block on suspicious account activities like:

- AAD Identity Protection: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
- Microsoft Defender for Cloud: https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction
- Microsoft Defender for Identity: https://docs.microsoft.com/en-us/defender-for-identity/what-is

It will allow you to quickly detect and (automatically) act on an account which may have been compromised.

Finally, it is also a good practice to create "Cost alerts" to get alerted as soon as possible on an unexpected consumption/cost increase: https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/cost-mgt-alerts-monitor-usage-spending

Mit freundlichen Grüßen,
Matthias Meiling

**Matthias Meiling**
Security Support Escalation Engineer
Cybersecurity Incident Response Team (MS-CIRT)
Microsoft Corporation

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München



Schedule: EMEA business hours (Mo. – Fr.) | For critical situations, in case you need any help outside of my shift, please reach out to azurebu@microsoft.com.
If you have any feedback about my work, please let either myself or my manager Gabor Gyori know at Gabor.Gyori@microsoft.com.



---------- Original Message ----------
**From:** frank.fuchs@ksv-fuchs.de;
**Received:** Mon Oct 02 2023 11:32:20 GMT+0200 (Central European Summer Time)
**To:** supportmail@microsoft.com;
**Subject:** WG: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

**Von:** KSV Fuchs | F. Fuchs
**Gesendet:** Montag, 2. Oktober 2023 11:27
**An:** 'kunden@microsoft.com' <kunden@microsoft.com>
**Cc:** 'support@microsoft.com' <support@microsoft.com>
**Betreff:** WG: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169 - Achtung Fristsache
**Priorität:** Hoch

… unsere Mail wurde von Microsoft ungelesen gelöscht???

Mir fehlen nur noch die Worte !!!!!!!!!

**Von:** KSV Fuchs | F. Fuchs
**Gesendet:** Montag, 2. Oktober 2023 11:18
**An:** 'supportmail@microsoft.com' <supportmail@microsoft.com>
**Betreff:** WG: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169 - Achtung Fristsache
**Priorität:** Hoch

**Sehr geehrte Damen und Herren,**

über Ihren Mitarbeiter, Herrn Klaus Bassler, wurde am 29.09.2023, die nachfolgende E-Mail inkl. vorausgehendem, problembezogenen E-Mail-Schriftwechsel an Sie übermittelt.

**Mit dem Vermerk:** *„Dass ist ein AAA Plus Problem und ich bitte um Erläuterung und Erklärung dieses Problemes, dringend!“* und der ersten Mitteilung hierzu vom 28.08.2023, ist die erneut ausgebliebene Reaktion von Microsoft, in unseren Augen als nicht hinnehmbar zu bezeichnen.

Über Ihr Azur Portal, nehmen Sie billigend in Kauf, dass ein Identitätsdiebstahl stattgefunden hat. Sie reagieren nicht auf unsere Anschreiben und auch die Reaktion mit entsprechenden Hinweisen Ihres Mitarbeiter Klaus Bassler, lässt Sie nicht dazu übergehen, an dieser immer noch vorherrschenden Situation etwas zu ändern.

Sie verletzten damit unsere Schutzrechte und nehmen es damit billigend in Kauf, dass neben dem uns entstanden Schaden, zusätzlich Datenschutzrechte verletzt werden könnten.
Auch das Lahmlegen unseres Firmenrechners durch Ihren Supportmitarbeiter, scheint Microsoft nicht im Geringsten zu interessieren.

Wir erwarten nach über 2 Monaten, eine umgehende Beseitigung dieser für uns unerträglichen Situation von ihnen, als verantwortlichen Portalbetreiber des Cloud Computing Services | Microsoft Azure.

**Hierfür setzen wir Ihnen eine Frist bis zum 05.10.2023. Sollten** Sie bis zu diesem Zeitpunkt immer noch zulassen, dass die Domain Coldbull.microsoft.de, ohne unsere Genehmigung von unberechtigten Dritten verwendet wird, werden wir die Angelegenheit an unseren Rechtsanwalt weiterleiten und unsere Erfahrungen mit der Öffentlichkeit teilen.

**Auszug der E-Mail von Herrn Klaus Bassler:**

**Wir hoffen nicht, dass wir diese Schritte gehen müssen und verbleiben**

**Frank Fuchs**
Kreditsachverständiger

Kontakt
Ludwig-Erhard-Allee 10
76131 Karlsruhe

Tel.: +49 (0)721 4807 4650

E-Mail: f.fuchs@ksv-fuchs.de
Website: https://ksv-fuchs.de/

USt.-ID: DE288421884

**Mitglied beim Bundesverband Deutscher Sachverständiger und Fachgutachter e.V.**



**Von:** Klaus Bassler <klausba@MICROSOFT.com>
**Gesendet:** Freitag, 29. September 2023 11:32
**An:** KSV Fuchs | F. Fuchs <frank.fuchs@ksv-fuchs.de>
**Cc:** Microsoft Support <supportmail@microsoft.com>; Klaus Bassler <klausba@MICROSOFT.com>
**Betreff:** RE: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrte Frau Adam, sehr geehrter Herr Fuchs,

wie eben telefonisch besprochen leite Ich Ihr Anliegen an unser Security Team weiter.

Zusammenfassung (um sicher zu gehen, dass der nächste Kollege nicht am Verständnis der Problematik scheitert, habe ich diese gleich auf Englisch zusammengefasst.
Ich hoffe, dass das für Sie so in Ordnung ist.) :

Customer still need to understand who created the Domain on their account Coldbull.onmicrosoft.com, even so they didn't request such a domain!
Please get in touch with the customer and assist with removing unexpected permissions for their account / clarify how to unsubscribe the whole account.

Coldbull.onmicrosoft.com is the initial domain name that the customer signed up with.

Still unclear:

1) Why do they see any security concern?

*„In unserem Konto wurde eine Domain eingetragen, die uns nicht gehört und die es offensichtlich auch nicht gibt. http://coldbull.onmicrosoft.com/ Das Thema wurde schon zig mal von uns angezeigt, aber Microsoft gelingt es offensichtlich nicht, diesen Fehler zu beheben.*
*Dass ist ein AAA Plus Problem und ich bitte um Erläuterung und Erklärung dieses Problemes, dringend!"*

2) What is the indicator that the die Domain Coldbull.microsoft.de has been created on their account?
Customer assumes that this is caused by this company:
BroadcastX GmbH
CEO: Manuel Wimmer

See attachments:
„Rechnung_RE-1472_11.07.2023 - Supportvertrag für 6 Monate ZinsId.pdf"
„Mail vom 20.08.2023 an Manuel Wimmer – Administrator.pdf"

==========

Ich hoffe Ihnen kann in der Sache nun auch wirklich weitergeholfen werden.

Sollte dies nicht der Fall sein, dürfen Sie sich gerne noch einmal Ende Oktober bei mir zurückmelden.

Mit freundlichen Grüßen

**Klaus Baßler**
Support Escal Eng Emea
Eq-De Emea Gtsc Dev Dsi
Customer Services and Support
Office: +49 (89) 31764552
klausba@microsoft.com

*Team Manager | Milton Pinto mpinto@microsoft.com +351 (21) 0602086*

Walter-Gropius-Straße 5, 80807 München
http://www.microsoft.com/germany
https://www.facebook.com/MicrosoftDE

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver | Amtsgericht München, HRB 70438

Microsoft is committed to protecting your privacy. Please read the Microsoft Privacy Statement for more information.
The above is an email for a support case from Microsoft Corp.
REPLY ALL TO THIS MESSAGE or INCLUDE casemail@microsoft.com IN YOUR REPLY if you want your response added to the case automatically.

Thank you.

**From:** Klaus Bassler <klausba@MICROSOFT.com>
**Sent:** Monday, September 25, 2023 2:24 PM
**To:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Cc:** Microsoft Support <supportmail@microsoft.com>; Gideon Omole (Tek Experts) <v-giomole@microsoft.com>; Klaus Bassler <klausba@MICROSOFT.com>
**Subject:** RE: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Fuchs,

leider konnte ich Sie auch heute telefonisch nicht erreichen.

Ihre Zusammenarbeit mit uns wäre hier essentiell und wichtig.

Sollten wir bis Mitte dieser Woche keine weitere Rückmeldung von Ihrer Seite erhalten, werden wir die Anfrage archivieren. Wir helfen Ihnen gerne auch später weiter, wenn Sie Zeit für dieses Thea haben.

Hierzu öffnen Sie dann bitte einfach eine neue Support Anfrage, mit Referenz auf diese hier.

Bis dahin verbleibe ich mit freundlichen Grüßen

**Klaus Baßler**
Support Escal Eng Emea
Eq-De Emea Gtsc Dev Dsi
Customer Services and Support
Office: +49 (89) 31764552
klausba@microsoft.com

*Team Manager | Milton Pinto mpinto@microsoft.com +351 (21) 0602086*

Walter-Gropius-Straße 5, 80807 München
http://www.microsoft.com/germany
https://www.facebook.com/MicrosoftDE

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver | Amtsgericht München, HRB 70438

Microsoft is committed to protecting your privacy. Please read the Microsoft Privacy Statement for more

information.
The above is an email for a support case from Microsoft Corp.
REPLY ALL TO THIS MESSAGE or INCLUDE casemail@microsoft.com IN YOUR REPLY if you want your response added to the case automatically.

Thank you.

**From:** Klaus Bassler
**Sent:** Thursday, September 14, 2023 9:48 AM
**To:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Cc:** Microsoft Support <supportmail@microsoft.com>; Gideon Omole (Tek Experts) <v-giomole@microsoft.com>; Gideon Omole (Tek Experts) <v-giomole@microsoft.com>
**Subject:** RE: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Fuchs,

leider konnte ich Sie telefonisch nicht erreichen, um mit Ihnen das weitere Vorgehen zu besprechen.

Bitte schicken Sie uns die Information, die mein Kollege Gideon bereits angefragt hat:

Verwalten einer Azure-Supportanfrage - Azure supportability | Microsoft Learn
*Sammeln erweiterter Diagnoseinformationen zulassen*
*Wenn Sie eine Supportanfrage erstellen, können Sie im Abschnitt Erweiterte Diagnoseinformationen entweder Ja oder Nein au*
*Diese Option bestimmt, ob der Azure-Support Diagnoseinformationen zu Ihrer Azure-Ressourcen, zum Beispiel Protokolldateie*
*kann, die möglicherweise zur Behebung Ihres Problems beitragen. Der Azure-Support kann nur dann auf erweiterte Diagnoseinformationen zugreifen, wenn Ihr Fall über das Azure-Portal erstellt wurde und Sie die Erlaubnis dazu erteilt haben.*

*So ändern Sie Ihre Auswahl bei Erweiterte Diagnoseinformationen, nachdem die Anforderung erstellt wurde:*

*Wählen Sie auf der Seite Alle Supportanfragen die Supportanfrage aus.*
*Wählen Sie auf der Seite Supportanfrage am oberen Rand des Bildschirms die Option Erweiterte Diagnoseinformationen aus.*
*Wählen Sie Ja oder Nein und dann Absenden aus.*

*Hochladen von Dateien*
*Sie können mithilfe der Dateiupload-Option eine Diagnosedatei, z. B. die Ablaufverfolgung des Browsers, oder andere Dateien die Sie als relevant für eine Supportanfrage erachten.*

*Wählen Sie auf der Seite Alle Supportanfragen die Supportanfrage aus.*
*Wählen Sie auf der Seite Supportanfrage das Feld Datei hochladen aus, navigieren Sie dann zu Ihrer Datei, und wählen Sie Hoc*

Ohne diese können wir Ihnen in der Sache nicht wirklich weiterhelfen.

Ich bin ab morgen bis einschließlich Mittwoch nicht im Hause.

Sollten wir bis Mitte nächster Woche nichts weiter von Ihnen hören, werden wir die Anfrage archivieren.
Wir helfen Ihne gerne auch später weiter, wenn Sie wieder an diesem Thema mit uns zusammenarbeiten können.

Bis dahin verbleibe ich mit freundlichen Grüßen

**Klaus Baßler**
Support Escal Eng Emea
Eq-De Emea Gtsc Dev Dsi
Customer Services and Support
Office: +49 (89) 31764552
klausba@microsoft.com

*Team Manager | Milton Pinto mpinto@microsoft.com +351 (21) 0602086*

Walter-Gropius-Straße 5, 80807 München
http://www.microsoft.com/germany
https://www.facebook.com/MicrosoftDE

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver | Amtsgericht München, HRB 70438



Thank you.

**From:** Klaus Bassler <klausba@MICROSOFT.com>
**Sent:** Monday, September 11, 2023 10:19 AM
**To:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Cc:** Microsoft Support <supportmail@microsoft.com>; Gideon Omole (Tek Experts) <v-giomole@microsoft.com>; Gideon Omole (Tek Experts) <v-giomole@microsoft.com>; Klaus Bassler <klausba@MICROSOFT.com>
**Subject:** RE: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Fuchs,

können uns bitte die Information zukommen lassen, die wir unten angefragt haben?

Ohne diese können wir Ihnen in der Sache nicht wirklich weiterhelfen.

Bis dahin verbleibe ich mit freundlichen Grüßen

**Klaus Baßler**
Support Escal Eng Emea
Eq-De Emea Gtsc Dev Dsi
Customer Services and Support
Office: +49 (89) 31764552
klausba@microsoft.com

*Team Manager | Milton Pinto mpinto@microsoft.com +351 (21) 0602086*

Walter-Gropius-Straße 5, 80807 München
http://www.microsoft.com/germany
https://www.facebook.com/MicrosoftDE

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver | Amtsgericht München, HRB 70438

Microsoft is committed to protecting your privacy. Please read the Microsoft Privacy Statement for more information.
The above is an email for a support case from Microsoft Corp.
REPLY ALL TO THIS MESSAGE or INCLUDE casemail@microsoft.com IN YOUR REPLY if you want your response added to the case automatically.

Thank you.

**From:** Klaus Bassler
**Sent:** Wednesday, September 6, 2023 12:40 PM
**To:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Cc:** Microsoft Support <supportmail@microsoft.com>; Gideon Omole (Tek Experts) <v-giomole@microsoft.com>; Gideon Omole (Tek Experts) <v-giomole@microsoft.com>
**Subject:** RE: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Fuchs,

können uns bitte noch diese offenen Fragen bitte beantworten?

Ebenso hat mein Kollege Gideon Ihnen diese Anleitung geschickt, um „advanced diagnostic information“ einzusammeln:

*“I understand that you have concerns about why a domain called Coldbull.microsoft.de has been registered in your tenant.*
*To keep investigating your support request #2308250050003169, we need to collect advanced diagnostic information.*

*Please allow permission to collect advanced diagnostic information via the Azure Portal.*

*Please do not hesitate to contact me should you require further information.”*

Können Sie uns diese Informationen liefern?

Bis dahin verbleibe ich mit freundlichen Grüßen

**Klaus Baßler**
Support Escal Eng Emea
Eq-De Emea Gtsc Dev Dsi
Customer Services and Support
Office: +49 (89) 31764552
klausba@microsoft.com

*Team Manager | Milton Pinto mpinto@microsoft.com +351 (21) 0602086*

Walter-Gropius-Straße 5, 80807 München
http://www.microsoft.com/germany
https://www.facebook.com/MicrosoftDE

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver |

Amtsgericht München, HRB 70438

Microsoft is committed to protecting your privacy. Please read the Microsoft Privacy Statement for more information.
The above is an email for a support case from Microsoft Corp.
REPLY ALL TO THIS MESSAGE or INCLUDE casemail@microsoft.com IN YOUR REPLY if you want your response added to the case automatically.

Thank you.

**From:** Klaus Bassler <klausba@MICROSOFT.com>
**Sent:** Friday, September 1, 2023 9:20 AM
**To:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Cc:** Klaus Bassler <klausba@MICROSOFT.com>; Microsoft Support <supportmail@microsoft.com>
**Subject:** RE: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Fuchs,

können uns bitte noch diese offenen Fragen bitte beantworten?

1) Woran erkenn Sie, dass bei Ihrer Umgebung 10 Sicherheitsrisiken bestehen?

2) Woher leiten Sie ab, dass die Domain Coldbull.microsoft.de existiert und auf bzw. „für Sie“ angelegt wurde?

Ich würde dann die gesammelten Daten an unser Azure Billing Team weiterreichen.

Mit freundlichen Grüßen

Klaus Baßler
Support Escal Eng Emea
Eq-De Emea Gtsc Dev Dsi
Customer Services and Support
Office: +49 (89) 31764552

*Team Manager | Team Manager | Milton Pinto mpinto@microsoft.com +351 (21) 0602086*

Microsoft Deutschland GmbH | Walter-Gropius-Straße 5 | 80807 München
Microsoft – Offizielle Website
Home | News Center Microsoft
Datenschutzerklärung von Microsoft – Microsoft-Datenschutz

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver | Amtsgericht München, HRB 70438

Microsoft is committed to protecting your privacy. Please read the Microsoft Privacy Statement for more information.
The above is an email for a support case from Microsoft Corp.
REPLY ALL TO THIS MESSAGE or INCLUDE casemail@microsoft.com IN YOUR REPLY if you want your response added to the case automatically.

Thank you.

**From:** Klaus Bassler <klausba@MICROSOFT.com>
**Sent:** Wednesday, August 30, 2023 4:54 PM
**To:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Cc:** Klaus Bassler <klausba@MICROSOFT.com>
**Subject:** RE: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Fuchs,

ja, die sieht in der Tat etwas verwirrend aus.
Können Sie mir die unten gestellten Fragen bitte beantworten?

Bis dahin bedanke ich mich for Ihre Geduld und verbleibe mit freundlichen Grüßen

Klaus Baßler
Support Escal Eng Emea
Eq-De Emea Gtsc Dev Dsi
Customer Services and Support
Office: +49 (89) 31764552

*Team Manager | Team Manager | Milton Pinto mpinto@microsoft.com +351 (21) 0602086*

Microsoft Deutschland GmbH | Walter-Gropius-Straße 5 | 80807 München
Microsoft – Offizielle Website
Home | News Center Microsoft
Datenschutzerklärung von Microsoft – Microsoft-Datenschutz

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver | Amtsgericht München, HRB 70438



Thank you.

**From:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Sent:** Wednesday, August 30, 2023 4:32 PM
**To:** Klaus Bassler <klausba@MICROSOFT.com>
**Cc:** RA Rohn - Dillerup & Rohn Rechtsanwälte <rohn@dr-rechtsanwaelte.de>
**Subject:** AW: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Bassler,

undurchsichtig finde ich das ganze allerdings auch. Im Anhang finden Sie die Rechnung, auf die der von mir beauftragte Dienstleister, ohne mein Wissen diese Domain angelegt hat.
Nachfolgend sehen Sie meine Unternehmensdaten in der Signatur. Hieraus können Sie sehen, dass diese Bestellung nicht passt.

Wir lassen alles aktuell von einem Rechtsanwalt und einer Fachfirma überprüfen und melden uns, wenn feststeht, wie dieses Desaster zustande gekommen ist.

Mit freundlichen Grüßen

**Frank Fuchs**
Kreditsachverständiger

Kontakt
Ludwig-Erhard-Allee 10
76131 Karlsruhe

Tel.: +49 (0)721 4807 4650

E-Mail: f.fuchs@ksv-fuchs.de
Website: https://ksv-fuchs.de/

USt.-ID: DE288421884

**Mitglied beim Bundesverband Deutscher Sachverständiger und Fachgutachter e.V.**



---

**Von:** Klaus Bassler <klausba@MICROSOFT.com>
**Gesendet:** Mittwoch, 30. August 2023 16:14
**An:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Cc:** Klaus Bassler <klausba@MICROSOFT.com>; Microsoft Support <supportmail@microsoft.com>
**Betreff:** RE: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Fuchs,

es wird immer unklarer, welches Team tatsächlich helfen könnten.

Was ich bislang sehen:

Sie haben offensichtlich keine aktive Azure Subscription.

Aus dem einen Screenshot ist ersichtlich, dass Sie Microsoft Business 365 Standard im Einsatz haben (Microsoft Entra Admin Center).

Sie schreiben auch:

„Azure Konto wurde nicht von uns angelegt. Die Domain Domain Coldbull.microsoft.de gehört uns nicht„
*„für unsere Organisation wurde ein Azur Konto angelegt, aber nicht von uns. Ich bitte um Erläuterung, wie es dazu kommen kann.*
***In diesem Konto werden 10 Sicherheitsrisiken angezeigt?“***

1) Woran erkenn Sie, dass 10 Sicherheitsrisiken bestehen?

*„In unserem Konto wurde eine Domain eingetragen, die uns nicht gehört und die es offensichtlich auch nicht gibt. http://coldbull.onmicrosoft.com/ Das Thema wurde schon zig mal von uns angezeigt, aber Microsoft gelingt es offensichtlich nicht, diesen Fehler zu beheben.*
*Dass ist ein AAA Plus Problem und ich bitte um Erläuterung und Erklärung dieses Problemes, dringend!“*

2) Woher leiten Sie ab, dass die Domain Coldbull.microsoft.de existiert und auf bzw. „für Sie“ angelegt wurde?

Die beiden PDF Dateien die Sie uns geschickt haben:
„Rechnung_RE-1472_11.07.2023 - Supportvertrag für 6 Monate ZinsId.pdf“
„Mail vom 20.08.2023 an Manuel Wimmer – Administrator.pdf“

Daraus erkenne ich keine für dieses Ticket hilfreiche Informationen.

Wenn wir diese Informationen haben, kann ich versuchen das entsprechend weiterzuleiten.

Bis dahin bedanke ich mich for Ihre Geduld und verbleibe mit freundlichen Grüßen

Klaus Baßler
Support Escal Eng Emea
Eq-De Emea Gtsc Dev Dsi
Customer Services and Support
Office: +49 (89) 31764552

*Team Manager | Team Manager | Milton Pinto mpinto@microsoft.com +351 (21) 0602086*

Microsoft Deutschland GmbH | Walter-Gropius-Straße 5 | 80807 München
Microsoft – Offizielle Website
Home | News Center Microsoft
Datenschutzerklärung von Microsoft – Microsoft-Datenschutz

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver | Amtsgericht München, HRB 70438



Thank you.

**From:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Sent:** Tuesday, August 29, 2023 5:46 PM
**To:** Klaus Bassler <klausba@MICROSOFT.com>
**Subject:** AW: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Baßler,

im Anhang Screenshot …

**Von:** Klaus Bassler <klausba@MICROSOFT.com>
**Gesendet:** Dienstag, 29. August 2023 14:14
**An:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Cc:** Klaus Bassler <klausba@MICROSOFT.com>
**Betreff:** RE: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Fuchs,

vielen Dank für Ihre Rückmeldung.

Der Screenshot beschreibt ein Microsoft 365 Business Standard Konto, das soweit ich weiß nicht mit dem Azure Konto zusammenhängen muss.
Wenn Sie sich unter https://portal.azure.com/ mit ihrem Konto anmelden, sollten Sie unter

Subscriptions - Microsoft Azure

die Subscription ID sehen.
Ist f.fuchs@ksv-fuchs.de der Account, mit der Sie sich dort anmelden?

Mit freundlichen Grüßen

Klaus Baßler
Support Escal Eng Emea
Eq-De Emea Gtsc Dev Dsi
Customer Services and Support
Office: +49 (89) 31764552

*Team Manager | Team Manager | Milton Pinto mpinto@microsoft.com +351 (21) 0602086*

Microsoft Deutschland GmbH | Walter-Gropius-Straße 5 | 80807 München
Microsoft – Offizielle Website
Home | News Center Microsoft
Datenschutzerklärung von Microsoft – Microsoft-Datenschutz

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver | Amtsgericht München, HRB 70438



Thank you.

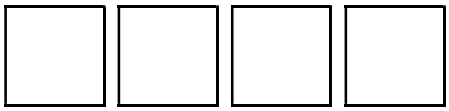
**From:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Sent:** Tuesday, August 29, 2023 1:13 PM
**To:** Klaus Bassler <klausba@MICROSOFT.com>
**Subject:** AW: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Baßler,

Im Anhang erhalten Sie einen Auszug von dem angemeldeten Konto. Die Adressdaten sind falsch, was ich bereits bei Microsoft reklamiert habe.

**Frank Fuchs**
**Sachverständiger für Kreditwesen, KSV Fuchs**

072148074650 | ksv-fuchs.de | info@ksv-fuchs.de
Ludwig-Erhard-Allee 10, 76131 Karlsruhe



**Von:** Klaus Bassler <klausba@MICROSOFT.com>
**Gesendet:** Dienstag, 29. August 2023 08:46
**An:** Microsoft Support <supportmail@microsoft.com>; Frank Fuchs <f.fuchs@ksv-fuchs.de>; Microsoft Support <supportmail@microsoft.com>
**Cc:** Klaus Bassler <klausba@MICROSOFT.com>
**Betreff:** RE: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Fuchs,

in der Problembeschreibung steht:

AzureProductSubscriptionID: No Subscription

Können Sie uns die Subscription ID und / oder die email Adresse liefern, auf die der entsprechende Account registriert ist, sowie der Account, von dem die Änderungen (Wimmer ?) vermeintlich vorgenommen wurde?

Mit freundlichen Grüßen

Klaus Baßler
Support Escal Eng Emea
Eq-De Emea Gtsc Dev Dsi
Customer Services and Support
Office: +49 (89) 31764552

*Team Manager | Team Manager | Milton Pinto mpinto@microsoft.com +351 (21) 0602086*

Microsoft Deutschland GmbH | Walter-Gropius-Straße 5 | 80807 München
Microsoft – Offizielle Website
Home | News Center Microsoft
Datenschutzerklärung von Microsoft – Microsoft-Datenschutz

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver | Amtsgericht München, HRB 70438

information.
The above is an email for a support case from Microsoft Corp.
REPLY ALL TO THIS MESSAGE or INCLUDE casemail@microsoft.com IN YOUR REPLY if you want your response added to the case automatically.

Thank you.

**From:** Klaus B <support@mail.support.microsoft.com>
**Sent:** Monday, August 28, 2023 4:15 PM
**To:** f.fuchs@ksv-fuchs.de; Microsoft Support <supportmail@microsoft.com>; Klaus Bassler <klausba@MICROSOFT.com>
**Subject:** RE: [EXTERNAL] AW: Azure Konto wurde nicht von ... - TrackingID#2308250050003169

Sehr geehrter Herr Fuchs,

mein Name ist Klaus Baßler, ich bin ein Support Escalation Engineer im Client apps and Services Developer Support Team zu dem Ihre Anfrage weitergeleitet wurde.

Auch das sollte so nicht passieren, genauso wie die Unannehmlichkeiten, die anscheinend an ihrem Azure Konto passieren.

Auch wenn ihre Anfrge bei unserem Team nicht wirklich richtig ist, werde Ich versuche nun Unterstützung vom entsprechenden richtigen Team anfordern, damit Ihnen in der Sache geholfen werden kann.

Bis dahin bedanke ich mit für Ihre Geduld und verbleibe mit freundlichen Grüßen

Klaus Baßler
Support Escal Eng Emea
Eq-De Emea Gtsc Dev Dsi
Customer Services and Support
Office: +49 (89) 31764552

*Team Manager | Team Manager | Milton Pinto mpinto@microsoft.com +351 (21) 0602086*

Microsoft Deutschland GmbH | Walter-Gropius-Straße 5 | 80807 München
Microsoft – Offizielle Website
Home | News Center Microsoft
Datenschutzerklärung von Microsoft – Microsoft-Datenschutz

Geschäftsführer*in: Dr. Marianne Janik (Vorsitzende), Florian Deter, Benjamin O. Orndorff, Keith Dolliver | Amtsgericht München, HRB 70438

Thank you.
---------- Original Message ----------
**From:** f.fuchs@ksv-fuchs.de;
**Received:** Mon Aug 28 2023 13:50:31 GMT+0200 (Central European Summer Time)
**To:** supportmail@microsoft.com;
**Subject:** [EXTERNAL] AW: Azure Konto wurde nicht von uns ... - TrackingID#2308250050003169

**Sehr geehrter Herr Anil Kumar,**

vielen Dank für Ihre Rückmeldung.

Wir haben uns schon mehrmals an dein Microsoft Support gewandt, wegen Problemen mit unserer E-Mail info@ksv-fuchs.de.

Im Anhang füge ich Ihnen eine E-Mail vom 20.08.2023 an einen von uns beauftragten Administrator, der ohne mein Wissen in Microsoft Azur angelegt hat.
Auf meine Reklamationen und Hinweise reagiert Herr Wimmer nicht. Auch auf die Anschreiben meines Rechtsanwaltes reagiert er nicht.

**Hier ein Screenshot von der Benutzerperson: support.braodcastx.altlassian.net.**

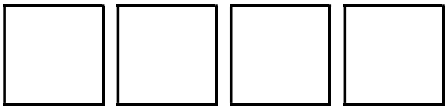
Bei der Domain „coldbull.onmicrosoft.com“, handelt es sich um eine Domain von einem Unternehmen, das nicht mehr existiert und auch nicht zu meiner Organisation gehört. Leider kann ich diese Domain, nicht löschen, weil diese Domain vom Ersteller mit höheren Rechten angelegt wurde.
Aus diesem Grund habe ich mich auch an den Microsoft Support gewandt, in der Hoffnung, dass Sie mir zurück zu meinen Daten und Eigentumsrechten verhelfen können.

Sollten Sie weitere Unterlagen von mir benötigen, bitte ich um einen entsprechenden Hinweis.

**Anlagen:**
E-Mail vom 20.08.2023 an den Geschäftsführer der Firma BroadcastX
Rechnung der Firma BroadcastX über Support meiner Domain app.ksv-fuchs.de mit der E-Mail zinsid@ksv-fuchs.de

**Frank Fuchs**
**Sachverständiger für Kreditwesen, KSV Fuchs**

072148074650 | ksv-fuchs.de | info@ksv-fuchs.de
Ludwig-Erhard-Allee 10, 76131 Karlsruhe



**Von:** Anil K <support@mail.support.microsoft.com>
**Gesendet:** Montag, 28. August 2023 09:35
**An:** Frank Fuchs <f.fuchs@ksv-fuchs.de>
**Betreff:** Azure Konto wurde nicht von uns angelegt. Die D... - TrackingID#2308250050003169

Hello Frank,

Greetings of the Day!

Thank you for contacting Microsoft Support.

My name is Anil Kumar Reddy Madhireddy. I am the Support Professional who will be working with you on this Service Request. You may reach me using the contact information listed below, referencing the SR number 2308250050003169. I'm reaching out about your request for help on the issue below:

**Stated Issue**: Azure account was not created by us. The domain Coldbull.microsoft.de does not belong to us.

Here's a possible sequence of events that could have led to the creation of an Azure account for your organization without your direct involvement:
1. **Employee Initiative:** An employee or a team within your organization might have felt the need for Azure services to support their projects or tasks.
2. **Lack of IT Involvement:** Due to perceived delays or bureaucracy in getting IT resources approved through official channels, the employee or team might have decided to create an Azure account independently.
3. **Creation of Azure Account:** Using their personal or departmental email addresses, they would have signed up for an Azure account using Microsoft's self-service sign-up process.
4. **Resource Deployment:** Once the account was set up, they could have started deploying resources such as virtual machines, storage, databases, etc., under that account to support their projects.
5. **Security Risks:** Without proper IT oversight, security practices might not have been adequately followed. This could result in potential security risks, misconfigurations, or unauthorized access to data.
6. **Inaccurate Information:** In the case of the domain "coldbull.onmicrosoft.com," it seems like an incorrect or non-existent domain was used during the setup. This could be a typo or an attempt at obfuscation.

It's important to address this situation promptly:

1. **Ownership**: Determine who created the account and which department or team is responsible.
2. **Security Assessment:** Since you've mentioned that there are 10 security risks associated with the account, it's crucial to assess these risks and address them immediately. Security risks could include misconfigured resources, exposed data, inadequate access controls, etc.
3. **Integration with IT**: Work to integrate the resources deployed in the shadow Azure account with the official IT infrastructure. This might involve migrating resources to an officially managed Azure subscription or tenant.
4. **Communication and Training**: Ensure that employees are aware of proper IT procedures and the risks associated with shadow IT. Provide clear communication channels for requesting IT resources.
5. **Audit and Monitoring:** Regularly audit and monitor the organization's IT resources to identify any unauthorized or shadow IT activities. Implement strong access controls and monitoring mechanisms.
6. **Data Cleanup**: If the "coldbull.onmicrosoft.com" domain doesn't belong to your organization, you should investigate its presence in your account. If it's not relevant, it should be removed or corrected.

Note that for further investigation on the case I'm transferring the ticket to respective team who were specialized on these areas. Please cooperate with us.

Awaiting your response.

Thank you,
Anil Kumar Reddy Madhireddy
Cloud Identity POD Support | *v-amadhiredd@microsoft.com
Working hours: Mon-Fri 12:00 PM – 09:30 PM (IST)