

Gefahren rund um die WM

wie Kriminelle Fußballfans ausnutzen





Kontakt Daten

ABOUT NIKOLAUS STAPELS

CYBERSECURITY ZUR WM 2026

Nikolaus Stapels ist Cybersecurity-Experte, VdS-Berater für Cyber-Security und begleitet Unternehmen, Versicherer und Vermittler bei der Bewertung und Reduzierung digitaler Risiken. In seinen Vorträgen verbindet er Praxiswissen aus Cyber-Schäden, Social Engineering und IT-Sicherheitsberatung mit verständlichen Beispielen aus dem Alltag.

Während der WM zeigt er, wie Cyberkriminelle die Begeisterung rund um Tickets, Streaming, Gewinnspiele und Fan-Angebote ausnutzen – und wie man sich wirksam davor schützt.





CYBERGEFAHREN ZUR WM 2026

WO MILLIONEN FANS KLICKEN, KLICKEN BETRÜGER MIT

Die Fußball-WM ist nicht nur ein Sportereignis, sondern ein globaler digitaler Ausnahmezustand: Tickets, Livestreams, Fan-Shops, Gewinnspiele und Social Media werden zur perfekten Angriffsfläche für Cyberkriminelle.



5 MRD.

Menschen interagierten mit Inhalten rund um die FIFA WM 2022.

1,5 MRD.

Menschen sahen weltweit das Finale der WM 2022.

93,6 MIO.

Social-Media-Posts zur WM 2022 erzeugten eine kumulative Reichweite von 262 Milliarden Kontakten.

ABOUT CYBER RISKS

WM 2026: DAS SPIELFELD DER CYBERKRIMINELLEN

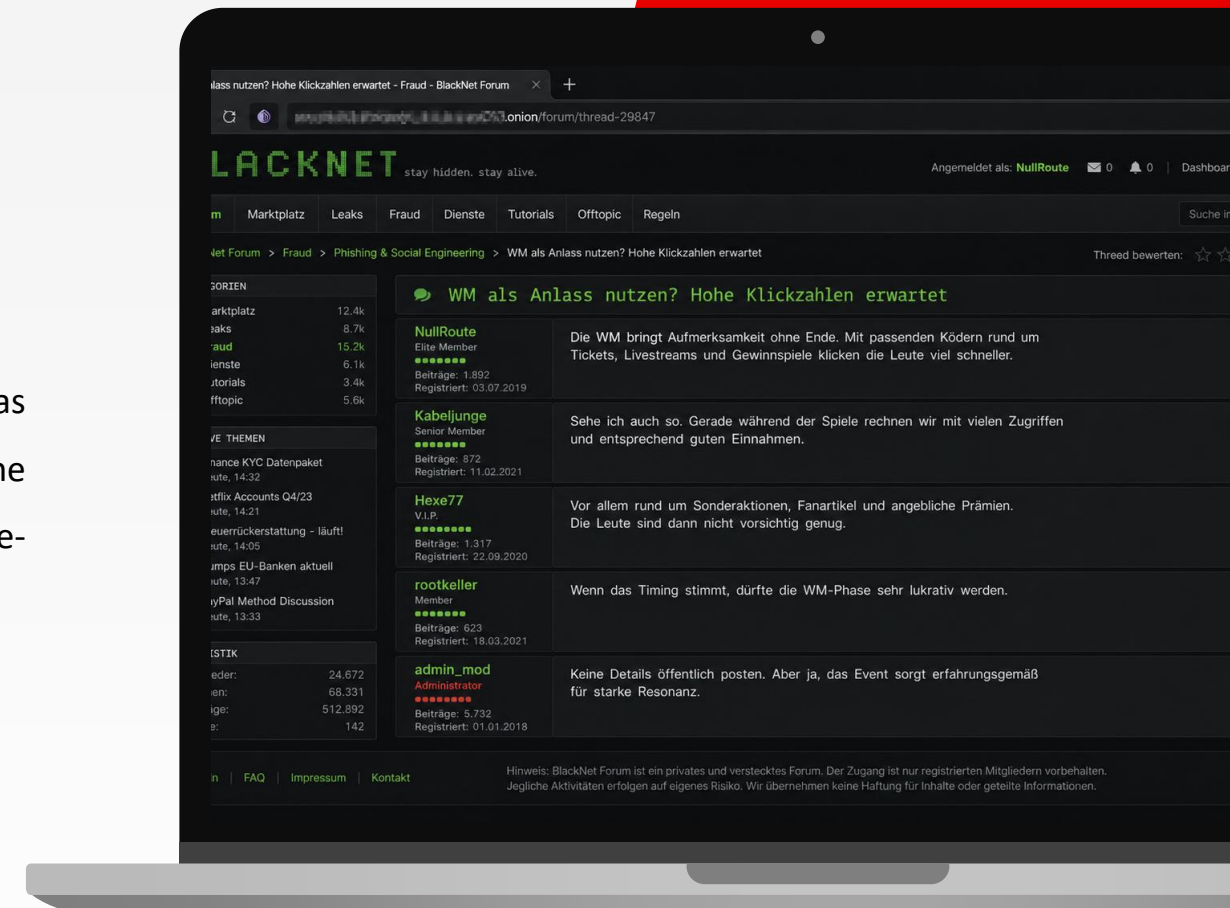
5 Milliarden Menschen interagierten mit Inhalten der WM 2022. Das Finale sahen rund 1,5 Milliarden Menschen weltweit. Diese enorme Aufmerksamkeit macht die WM zur idealen Bühne für Phishing, Fake-Tickets, Betrugs-Shops und manipulierte Streaming-Angebote.

PHISHING & FAKE-TICKETS

Kriminelle nutzen Vorfreude, Zeitdruck und ausverkaufte Spiele, um Fans auf gefälschte Webseiten zu locken.

FAKE-STREAMS & FAN-SHOPS

Angebliche Gratis-Streams und Sonderangebote führen häufig zu Datenklau, Zahlungsbetrug oder Schadsoftware.



WARUM DAS THEMA UNS ALLE BETRIFFT

DIE WM IST MEHR ALS FUSSBALL

Während der WM steigt nicht nur die Begeisterung, sondern auch die digitale Aktivität: Mitarbeitende suchen Tickets, klicken auf Gewinnspiele, streamen Spiele, bestellen Fanartikel oder nutzen öffentliche WLANs auf Reisen.

Genau diese Mischung aus Emotion, Zeitdruck und Aufmerksamkeit nutzen Cyberkriminelle gezielt aus. Für Gewerbekunden bedeutet das: Cyberrisiken entstehen nicht nur durch komplexe Hackerangriffe, sondern oft durch einen einzigen unüberlegten Klick im Arbeitsalltag.

FANS WERDEN ZU ZIELEN

Fake-Tickets, Phishing-Mails, gefälschte Streams und betrügerische Fan-Shops treffen Menschen genau dann, wenn sie schnell entscheiden wollen.

UNTERNEHMEN WERDEN MITGETROFFEN

Wenn Mitarbeitende private WM-Themen am Firmenrechner öffnen, können Zugangsdaten, Kundendaten und Unternehmenssysteme gefährdet werden.



☰

Neue E-Mail

Favoriten

Posteingang 12

Gesendet

Entwürfe 3

Papierkorb

Ordner +

Posteingang 12

Junk-E-Mail 28

Entwürfe 3

Gesendet

Gelöscht

Archiv

Notizen

Verlauf der Unterhaltung

Spamverdacht 4

Neuen Ordner erstellen

Suchen

RelevantSonstigeFilter

GW

Gewinnspiel-Service

Glückwunsch! Sie haben 2 WM-Karten für...

Sehr geehrte/r Gewinner/in, herzlichen Glückwunsch!...

18.05.2026

NK

Newsletter Aktuell

Die neuesten Angebote für Mai

Entdecken Sie unsere Top-Angebote diesen Monat.

17.05.2026

BS

Buchhaltung Service

Ihre Rechnung vom 17.05.2026

Anbei erhalten Sie Ihre Rechnung.

17.05.2026

TS

Team Support

Wichtige Informationen zu Ihrem Konto

Bitte überprüfen Sie Ihre Kontodaten.

16.05.2026

MR

Mein Reisebüro

Ihr Reisevorschlag für den Sommer

Traumhafte Ziele zu Top-Preisen.

16.05.2026

DA

Daily Deals

Nur heute: 20% Rabatt auf ausgewählte Artikel

Sichern Sie sich jetzt Ihr Angebot.

15.05.2026

SB

Service Benachrichtigungen

Wichtige Sicherheitsinformation

Informationen zur Sicherheit Ihres Kontos.

15.05.2026

Antworten

Allen antworten

Weiterleiten

Löschen

Archivieren

Junk-E-Mail

Glückwunsch! Sie haben 2 WM-Karten für das Halbfinale inkl. Flug gewonnen

GW

Gewinnspiel-Service

gewinnspiel-service@promo-events.com

An: Max Mustermann

18.05.2026 09:14

Sehr geehrte/r Gewinner/in,

herzlichen Glückwunsch! Im Rahmen unseres aktuellen Gewinnspiels wurden Sie für 2 WM-Karten für das Halbfinale inklusive Flug ausgewählt.

Alle weiteren Informationen zu Ihrem Gewinn, den Reisedaten und den nächsten Schritten finden Sie im beigefügten PDF-Anhang.

Bitte prüfen Sie das Dokument zeitnah.

Mit freundlichen Grüßen

Ihr Gewinnspiel-Service

Gewinninformationen_WM_Halbfinale.pdf

PDF-Datei • 245 KB

18°C Bewölkt

Suche

10:32 18.05.2026

DER MENSCHLICHE FAKTOR

EIN EINZIGER KLIICK KANN GENÜGEN

Viele Menschen hier würden diese Mail vermutlich misstrauisch prüfen oder sofort löschen.

„Die spannende Frage ist nicht, ob wir hier im Raum die Mail erkennen. Die spannende Frage ist: Gibt es in Ihrem Unternehmen eine Person, die an so einen Gewinn glaubt, den Anhang öffnet – vielleicht im Stress, zwischen zwei Terminen oder einfach aus Neugier? Denn für einen Angriff reicht nicht das ganze Unternehmen. Es reicht eine einzige Person.“

Genau das macht solche Angriffe so gefährlich!
Cyberkriminelle brauchen nicht alle.
Sie brauchen nur einen.

4 WEGE, WIE CYBERKRIMINELLE DIE WM AUSNUTZEN

Cyberangriffe rund um die WM wirken selten technisch kompliziert. Meist beginnen sie mit einfachen Tricks: einer verlockenden Mail, einem günstigen Angebot, einem kostenlosen Stream oder einer emotionalen Nachricht.

Genau diese vier Vorgehensweisen schauen wir uns jetzt genauer an.

WAS KANN WÄHREND DER WM PASSIEREN?

PHISHING

E-Mail, SMS,
WhatsApp

FAKE-SHOPS

Tickets, Reisen,
Fanartikel

FAKE-STREAMS

Gratis-Streams,
Downloads

SOCIAL ENGINEERING

Druck, Neugier,
Emotionen

ANGRIFFSWEG 1: PHISHING

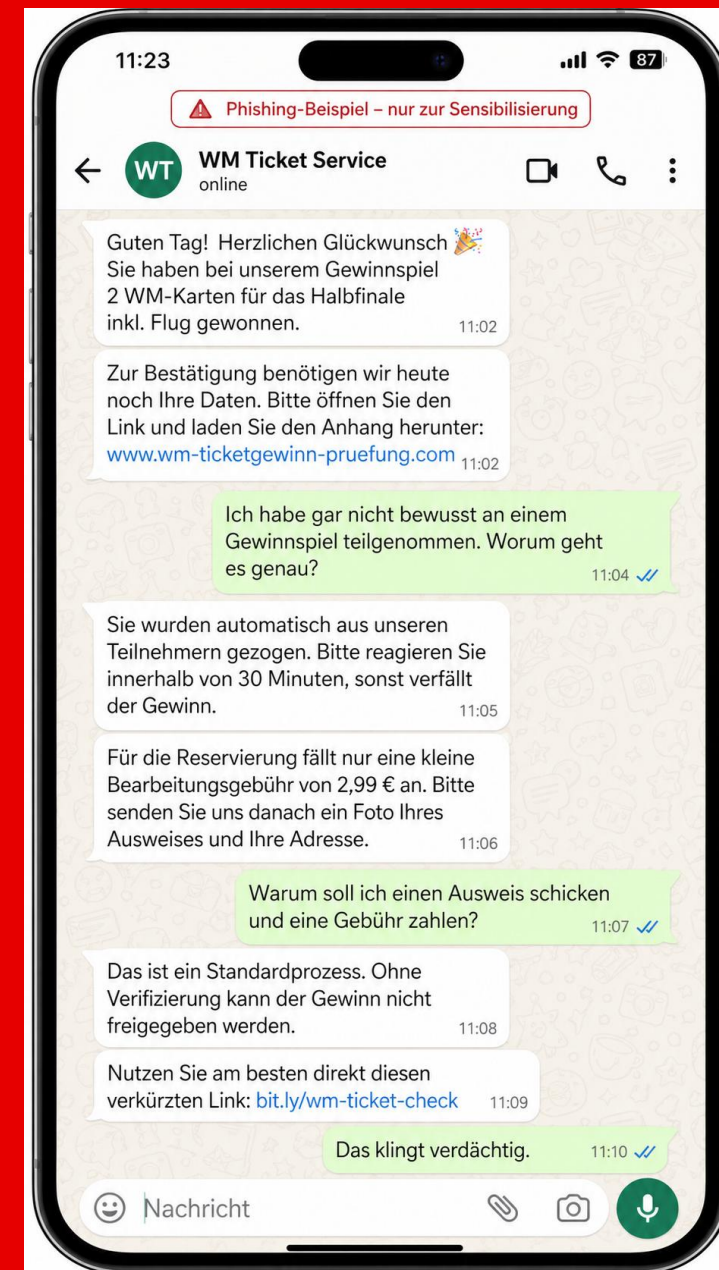
DER GEWINN, DEN ES NIE GAB

Zur WM nutzen Kriminelle gezielt die Vorfreude der Fans aus: angebliche Ticketgewinne, exklusive Fanpakete oder kurzfristige Reiseangebote wirken auf den ersten Blick verlockend. Über WhatsApp, SMS oder E-Mail werden Betroffene auf gefälschte Seiten gelockt.

Dort sollen sie persönliche Daten eingeben, Ausweisdokumente hochladen oder eine kleine „Bearbeitungsgebühr“ zahlen. Genau daraus entstehen Identitätsdiebstahl, Zahlungsbetrug oder der erste Zugang zu weiteren Angriffen.

WORAUF MAN ACHTEN SOLLTE

Ungewöhnlicher Absender, Zeitdruck, verkürzte Links, angebliche Gebühren, Upload von Ausweisfotos oder die Aufforderung, schnell zu reagieren.



ANGRIFFSWEG 2: FAKE-STREAMS

DER STREAM, DER ZUM RISIKO WIRD

Während der WM suchen viele Fans nach kostenlosen oder kurzfristig verfügbaren Livestreams. Genau das nutzen Kriminelle aus: Sie erstellen gefälschte Streaming-Seiten, die professionell aussehen und angeblich das Spiel live zeigen.

Kurz vor dem Start erscheint dann die Meldung: „**Für die Wiedergabe benötigen Sie ein Browser-Plugin**“ oder „**Bitte installieren Sie den HD-Player**“.

Wer diesem Hinweis folgt, installiert möglicherweise Schadsoftware, Adware oder eine Browser-Erweiterung, die Daten mitliest, Werbung einschleust oder Zugangsdaten abgreift.



chrome



Attention!
Your browser is out of date, some of extensions may interfere your work!



Please choose required update:

-  Chrome 23.1 SP1
-  Chrome 23.1 SP2
-  Chrome 23.1 SP2 + Antivirus protection
(recommended)

Current version of your browser is out of date (23.0.1271.64)

[Install](#)

mozilla Firefox



Attention!
Your browser is out of date, some of extensions may interfere your work!



Please choose required update:

-  Firefox 13.0 SP1
-  Firefox 13.0 SP2
-  Firefox 13.0 SP2 + Antivirus protection
(recommended)

Current version of your browser is out of date (10.0.2)

 [Install](#)

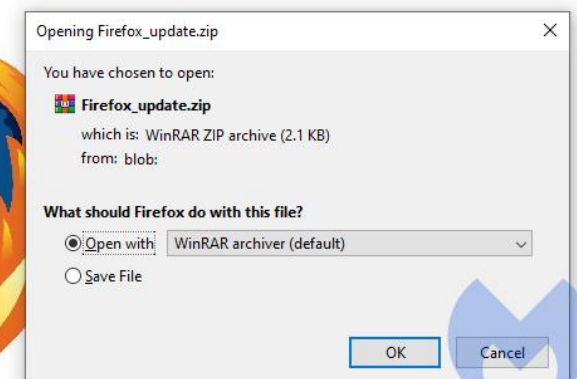
188.227.107.92/_cr/l/index.php

You firefox is ready for update

Your download should begin automatically.

Didn't work? Try downloading again.

[Upgrade my firefox](#)



AUSWIRKUNGEN FÜR UNTERNEHMEN

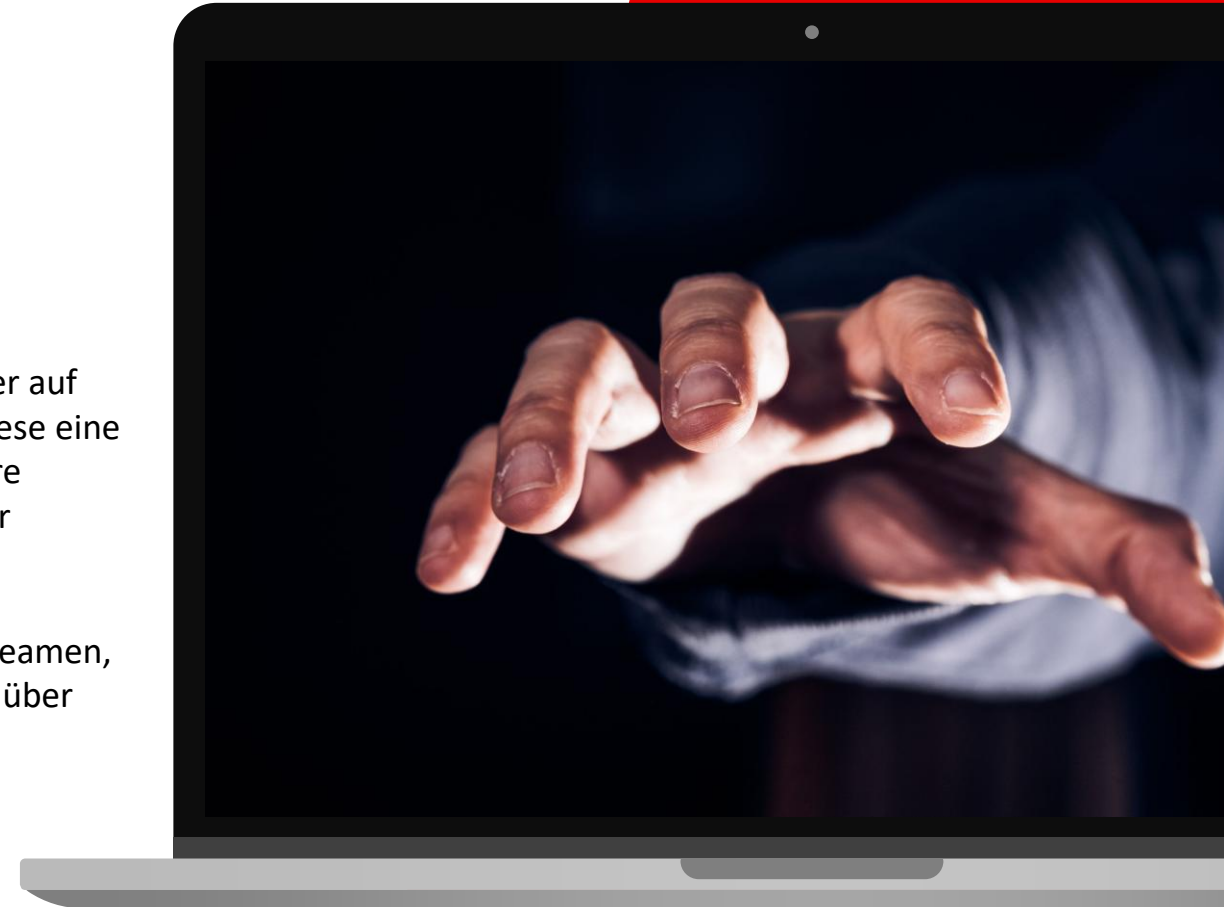
WENN EIN MITARBEITER DAS PLUGIN INSTALLIERT

Wird ein angebliches Browser-Plugin oder ein vermeintlicher Video-Player auf einem Unternehmensgerät installiert, bleibt der Schaden oft nicht auf diese eine Person beschränkt. Über manipulierte Erweiterungen oder Schadsoftware können Zugangsdaten abgegriffen, Browser-Sitzungen übernommen oder weitere Schadprogramme nachgeladen werden.

Damit wird aus einem scheinbar harmlosen Versuch, ein WM-Spiel zu streamen, schnell ein echtes Unternehmensrisiko: vom kompromittierten Endgerät über den Zugriff auf E-Mail-Konten bis hin zu Datenabfluss, Ransomware oder Störungen im Betriebsablauf.

MÖGLICHE FOLGEN:

Kontenübernahme, Datenabfluss, Ransomware, Betriebsunterbrechung.



ANGRIFFSWEG 3: FAKE-SHOPS

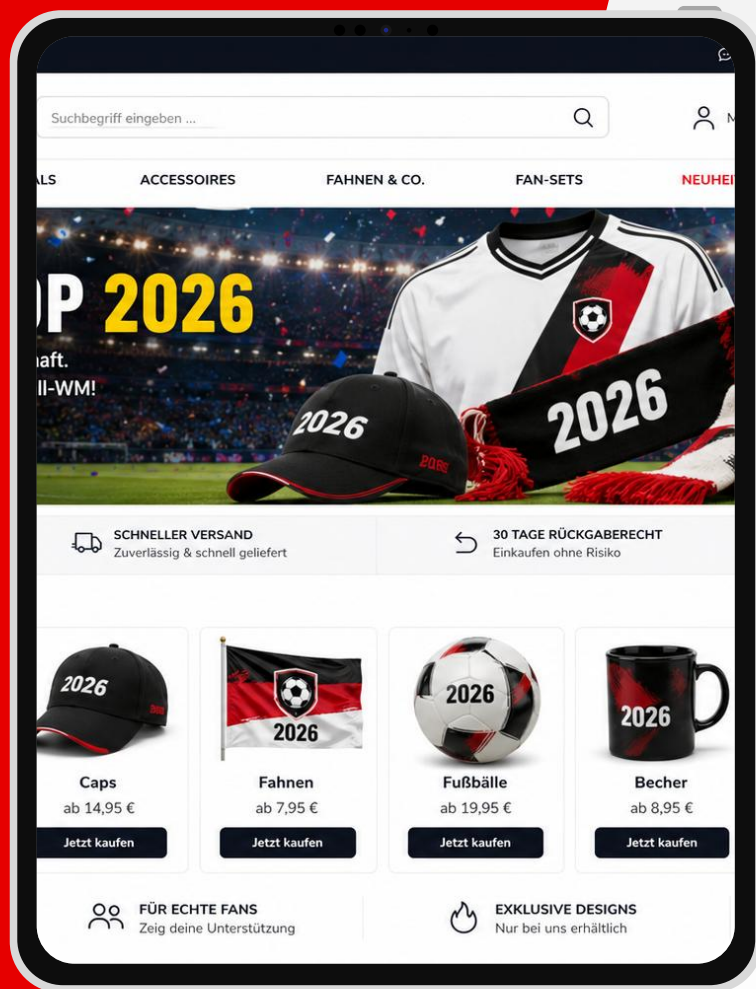
DER FAN-SHOP, DER KEINER IST

Zur WM entstehen zahlreiche gefälschte Online-Shops, die mit günstigen Trikots, limitierten Fanartikeln oder angeblich verfügbaren Tickets werben. Die Seiten wirken oft professionell, nutzen bekannte Logos, Countdown-Angebote und künstlichen Zeitdruck.

Für Unternehmen wird es problematisch, wenn Mitarbeitende solche Seiten während der Arbeitszeit über Firmenrechner besuchen. Dort können Zahlungsdaten abgegriffen, Zugangsdaten abgefragt, Schadcode über Werbenetzwerke geladen oder Mitarbeiter zu gefährlichen Downloads verleitet werden.

WARUM DAS GEFÄHRLICH IST

Ein Fake-Shop ist nicht nur ein privates Ärgernis. Auf Unternehmensgeräten kann der Besuch solcher Seiten zum Einfallstor für Datenklau, Malware, kompromittierte Browser-Sitzungen oder Reputationsschäden werden.



ANGRIFFSWEG 4: SOCIAL ENGINEERING

WENN NICHT DIE TECHNIK, SONDERN DER MENSCH ANGEGRIFFEN WIRD

Social Engineering bedeutet: Kriminelle greifen nicht zuerst Systeme an, sondern Menschen. Sie nutzen typische menschliche Reaktionen aus – Vorfreude, Hilfsbereitschaft, Unsicherheit, Stress oder Angst, etwas zu verpassen.

Gerade während der WM funktioniert das besonders gut! Tickets sind knapp, Angebote laufen angeblich ab, Gewinnbenachrichtigungen wirken emotional und Nachrichten sollen sofort beantwortet werden. So entsteht Druck – und genau unter Druck passieren Fehler.

1

DRUCK

Zeitlimit, knappe Verfügbarkeit und angebliche Konsequenzen sollen schnelles Handeln erzwingen.

2

NEUGIER

Gewinne, VIP-Zugänge oder geheime Angebote sollen dazu bringen, Links zu öffnen.

3

EMOTIONEN

Freude, Angst, Euphorie oder FOMO schalten den kritischen Blick aus.

REALITÄT AUS DER WM 2022

DAS PASSIERT NICHT NUR ANDEREN

Während der WM 2022 wurden zahlreiche Betrugs- und Phishing-Kampagnen entdeckt, gefälschte Ticketseiten, Fake-Streams, angebliche Gewinnspiele, betrügerische Fan-Shops und gefälschte Apps. Sicherheitsforscher fanden weltweit 16.000+ Phishing-Seiten, die gezielt darauf ausgelegt waren, persönliche Daten und Zahlungsinformationen von Fußballfans abzugreifen.

Für Unternehmen ist daran entscheidend: Die Betroffenen sind nicht nur „private Fans“, sondern auch Mitarbeitende, Führungskräfte und Unternehmer. Wer während der Arbeitszeit eine gefälschte WM-Seite besucht, einen Link öffnet oder Daten eingibt, kann unbeabsichtigt ein Unternehmensgerät, ein E-Mail-Konto oder Zugangsdaten gefährden.



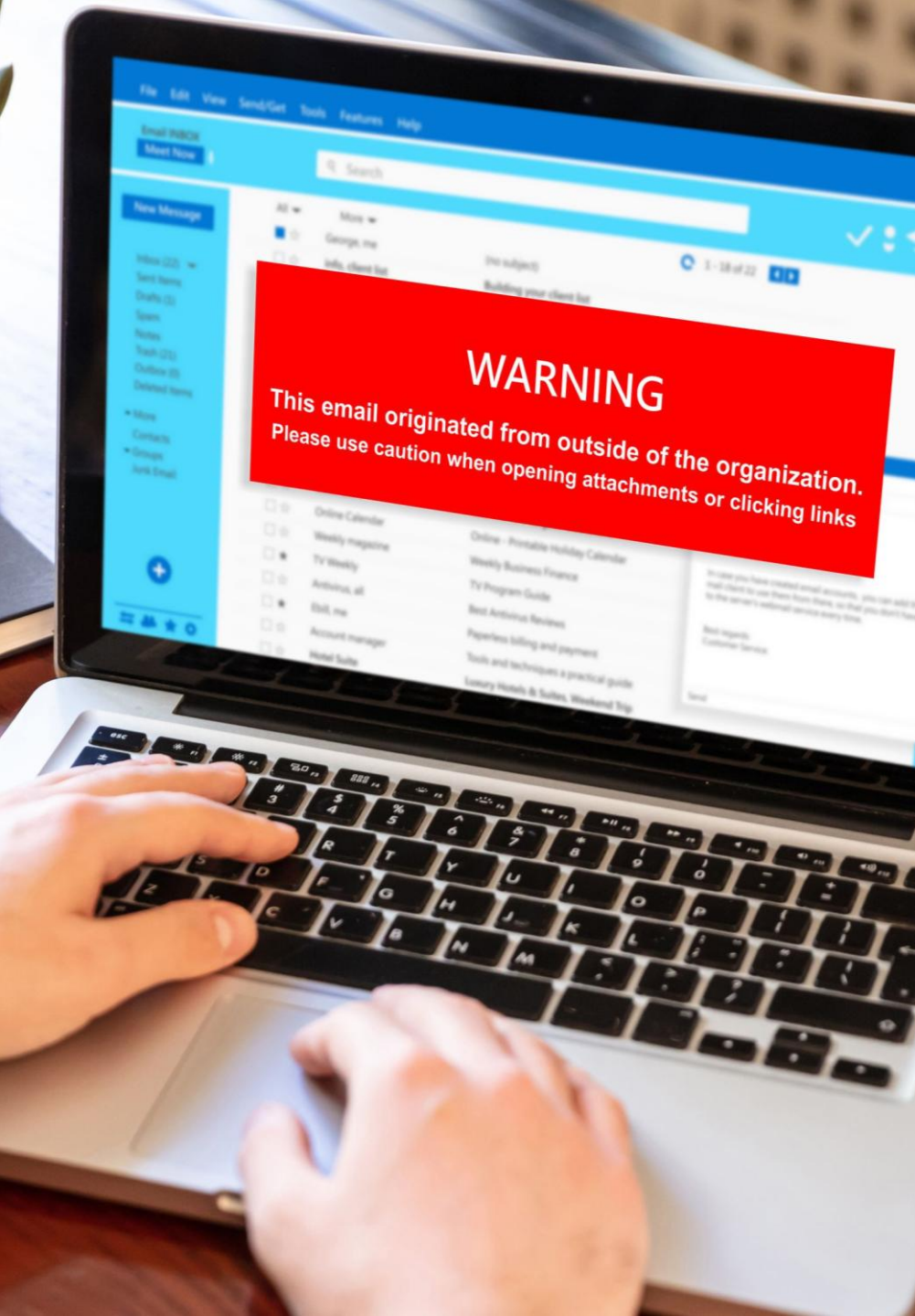
RISIKEN FÜR UNTERNEHMEN

WAS AUS EINEM EINZELNEN KLICK WERDEN KANN

Ein scheinbar harmloser Klick auf ein Ticketangebot, einen Fan-Shop oder einen Streaming-Link kann für Unternehmen weitreichende Folgen haben. Kriminelle zielen auf Zugangsdaten, Zahlungsinformationen, Geräte und interne Systeme. Besonders gefährlich ist, es genügt eine einzige Person im Unternehmen, damit ein Vorfall seinen Anfang nimmt.

Gefahren:

- Diebstahl von Zugangsdaten
- Schadsoftware auf Endgeräten
- Übernahme von E-Mail-Konten
- Manipulation von Browsern und Sitzungen
- Datenabfluss aus dem Unternehmen



AUSWIRKUNGEN FÜR DEN BETRIEB

WARUM UNTERNEHMEN SICH DAMIT BESCHÄFTIGEN MÜSSEN

Unternehmer müssen sich mit diesem Thema beschäftigen, weil aus privaten Klicks schnell betriebliche Schäden entstehen können. Ein Angriff kann den Arbeitsalltag stören, Kosten verursachen, Kundendaten gefährden und im schlimmsten Fall den Betrieb lahmlegen. Cyberkriminelle greifen nicht nur Technik an — sie nutzen Menschen im Unternehmen als Einfallstor.

Auswirkungen:

- Stillstand im Betrieb
- Finanzielle Schäden
- Vertrauensverlust bei Kunden
- Datenschutzprobleme
- Interner Aufwand
- Reputationsschaden

Kontakt

Nikolaus Stapels

 04551 - 5329578

 info@stapels.consulting



www.stapels.consulting

