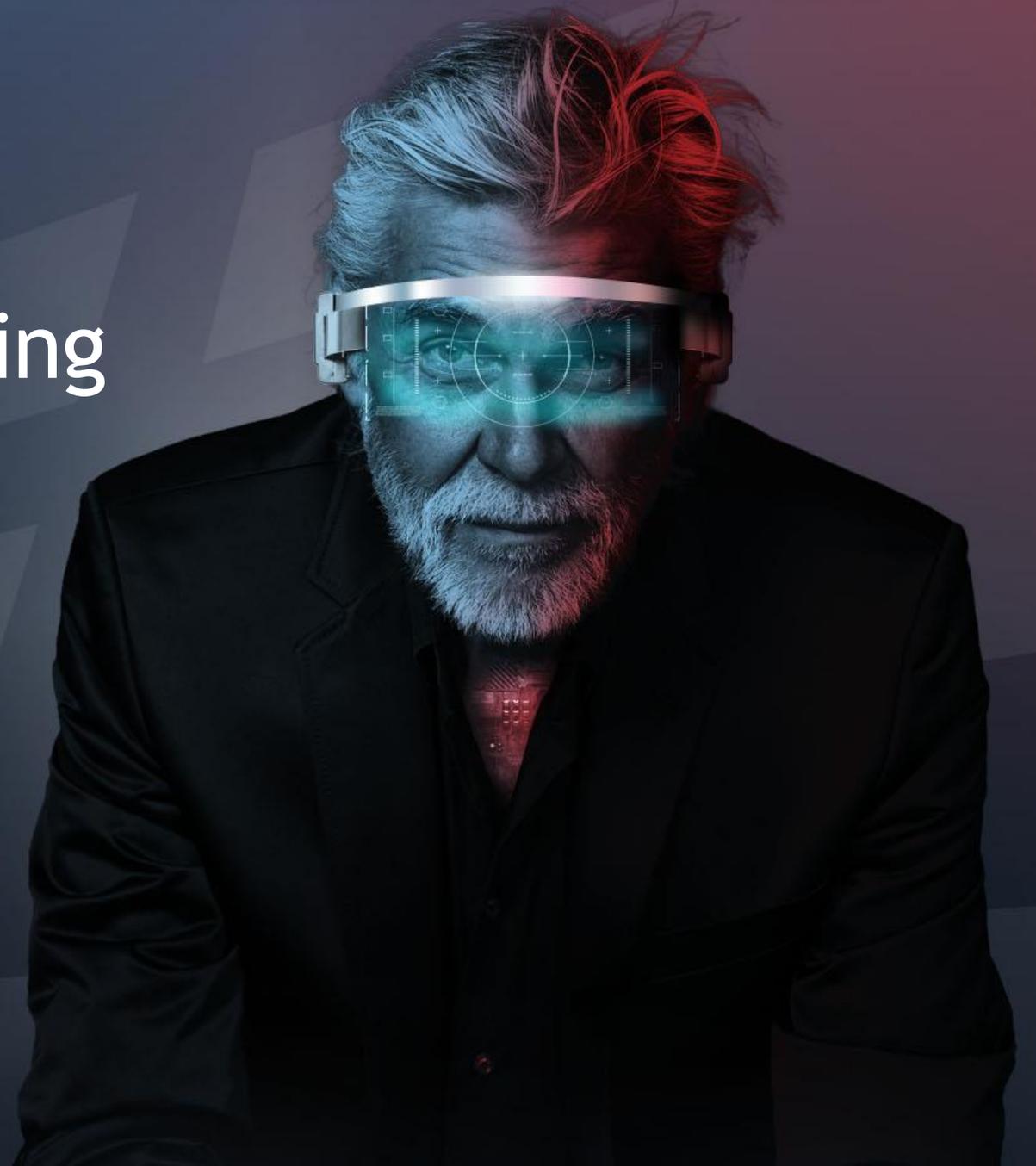


Demo Hack - Spear Phishing



DEUTSCHE GESELLSCHAFT FÜR
CYBERSICHERHEIT

AGENDA

Der Plan für heute

1. Vorstellung

2. Phishing

- Was ist Phishing?
- Statistik
- Spear Phishing

3. Demo Hack

- Überblick
- Vorbereitung
- Sicht des Opfers
- Sicht des Angreifers
- Zusammenfassung

4. Q&A

VORSTELLUNG

Speakers



Julian Geils

- Senior IT Security Consultant @DGC
- Previously IT Security Consultant and IT Security Engineer

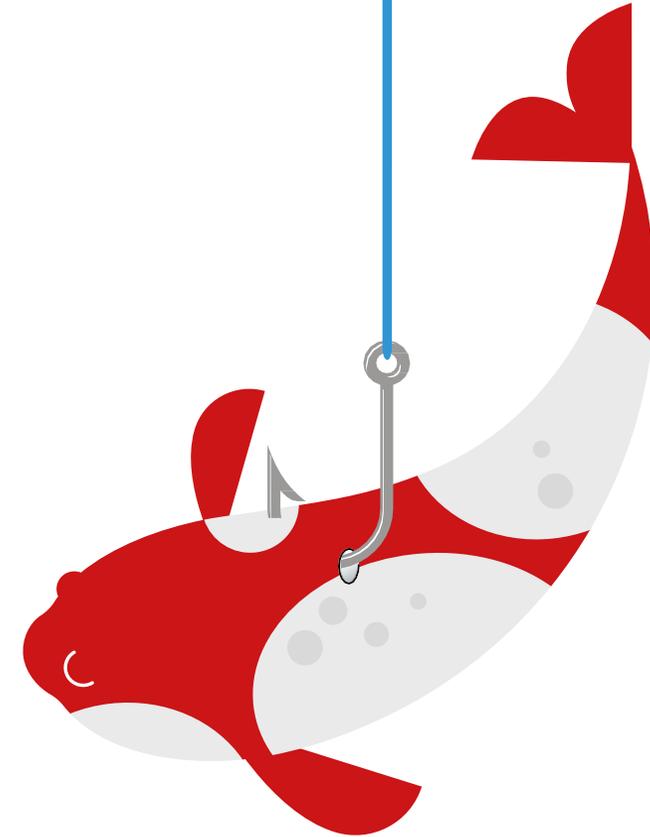
PHISHING

Was ist Phishing?

Phishing ist eine Form des **Trickbetruges**.

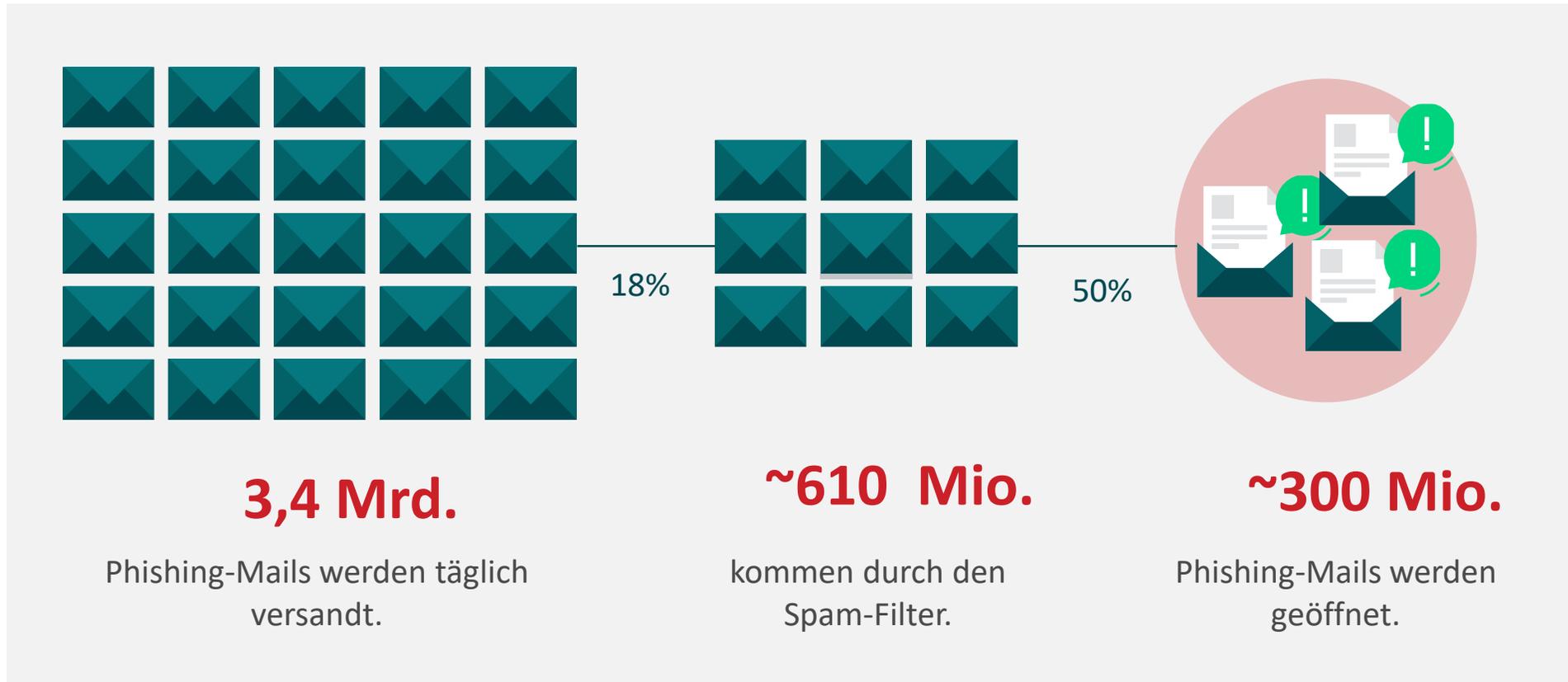
Angreifer erstellen **täuschend echte Nachrichten**.

Diese Nachrichten erzeugen **Druck, Vertrauen** oder vermeintlichen **Zugzwang** beim Empfänger.



PHISHING

STATISTIK

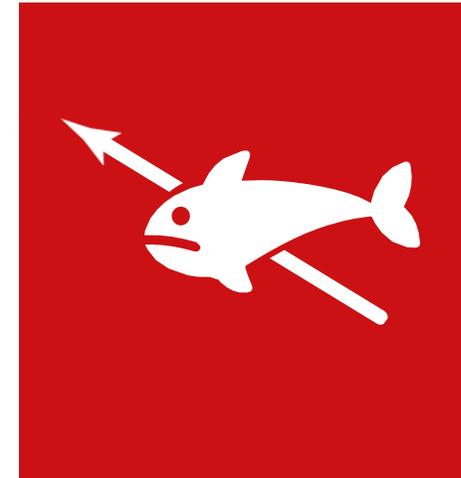


Quellen: Digital Shadows, Phish-Test-de; SoSafe Kundenprojekte 2018-2020

PHISHING

Spear Phishing

- Umfangreiche Vorbereitung
- Authentische Nachricht
- Dedizierte Zielgruppe



DEMO HACK

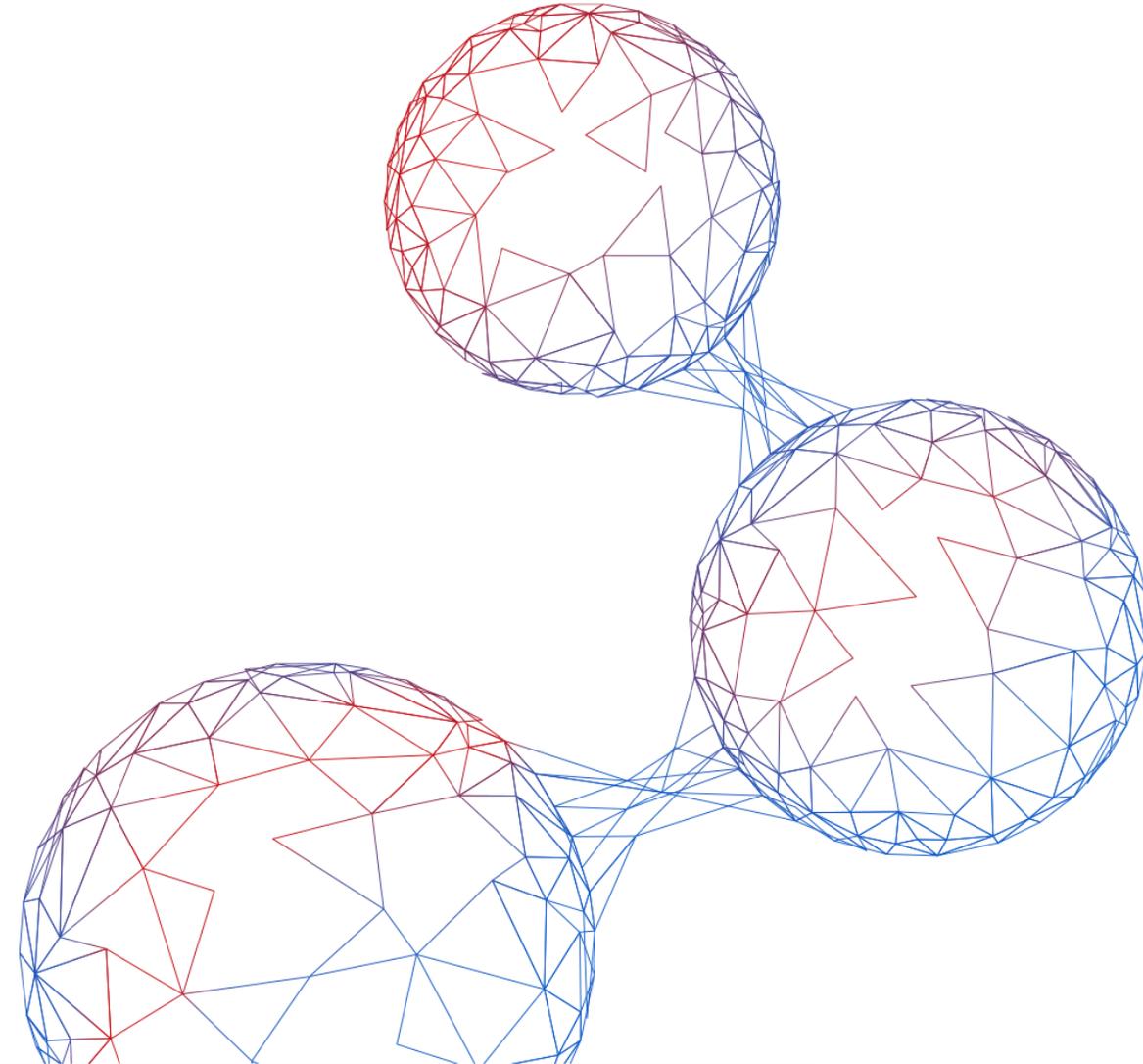
Überblick

Vorbereitung

- Bestimmt seine Zielgruppe
- Sucht einen Grund für seine Nachricht
- Macht Empfängeradressen ausfindig
- Eignet sich eine Absenderadresse an
- Erstellt die Nachricht samt Angriff

Ausführung

- Verschickt die Nachricht
- Wartet bis jemand den Angriff aktiviert
- Erhält Fernzugriff auf dem Rechner des Opfers
- Untersucht das System des Opfers



DEMO HACK

Vorbereitung



The screenshot shows the website for the Deutsche Gesellschaft für Cybersicherheit (DGC). The header includes the DGC logo, the text 'DEUTSCHE GESELLSCHAFT FÜR CYBERSICHERHEIT', and navigation links for 'Leistungen & Lösungen', 'News', 'Blog', 'Unternehmen', and 'Kontakt'. A search bar and a language selector set to 'DE' are also present. The main banner features a large eye graphic with a glowing blue and purple iris, overlaid with the text 'CyberInsights Der Blog rund um Ihre Datensicherheit'. Below the banner, there is a section titled 'Das DGC Sommerfest 2022' with a colorful geometric graphic and the text 'SOMMER FEST'. To the right, under 'Aktuelle Beiträge', there is an article titled 'Phishing Mails: Expertentipps für den Schutz vor Risiken' dated 29.08.2022. Below that, the 'Pressekontakt' section lists the 'Marketing Team' with phone number '+49 461 995838-32' and email 'marketing@dgc.org'. At the bottom left of the screenshot, the date '21.08.2022' and the URL 'https://dgc.org' are visible.



Vorbereitung

The screenshot shows the LinkedIn profile of Deutsche Gesellschaft für Cybersicherheit mbH & Co. KG. The profile banner features the company logo and the text "Wir managen die Risiken Ihrer digitalen Transformation". The company name is "Deutsche Gesellschaft für Cybersicherheit mbH & Co. KG", with the tagline "Computer- und Netzwerksicherheit". It is located in Flensburg, Schleswig-Holstein, and has 1,804 followers. A "Folgen" button is visible. Below the profile, a post by Olaf Opius, an IT Specialist at DGC, is partially visible. On the right side of the screenshot, the "Ähnliche Seiten" section lists several related organizations, including DGC International, DCSO Deutsche Cybersicherheitsorganisation, Bundesamt für Sicherheit in der Informationstechnik (BSI), and DGC in Stockholm. The "Jobs durchsuchen" section shows job listings for Marketing Manager-Jobs (16,448 free positions), Director-Jobs (81,262 free positions), and Analyst-Jobs (54,407 free positions).

Quelle: linkedin.com

DEMO HACK

Vorbereitung



Search **Finder** Verifier Bulks Leads Campaigns

Email Finder Author Finder

Email Finder

Olaf Opius @ dgc.org

olaf.opius@dgc.org + SAVE EMAIL

Olaf Opius
Deutsche Gesellschaft für Cybersicherheit mbH & Co. KG

We found this email address **once** on the web.

<http://dgc.org/random/article/fix-cve-details-for-yabb-xss-nasl-cve-...> Mar 01, 2022

Quelle: hunter.io

DEMO HACK

Vorbereitung

~~dgc.org~~

dgc.email

The screenshot shows the checkdomain website interface. At the top, there are five colored boxes (four red, one grey). The main header includes the checkdomain logo and a shopping cart icon. A search bar contains 'dgc.org' with a 'Multicheck' dropdown and a 'Neu checken' button. Below the search bar, there are filters for 'Alle Kategorien', 'Sortieren nach Beliebtheit', and a toggle for 'Nur freie Domains anzeigen' which is currently checked. A message states 'Deine Wunschdomain ist leider belegt.' for 'dgc.org', which is priced at 1,99 € im Monat and has an 'Umziehen' button. Under the heading 'Unsere Empfehlungen', a table lists several domain suggestions:

Domain	Status	Preis mtl.*	Action
dgc.email	✓ Noch frei!	2,49 €	Auswählen
dgc.app	Fehler		Domain ist zu kurz
dgc.blog	Fehler		Domain ist zu kurz
dgc.rocks	✓ Noch frei!	1,99 €	Auswählen
dgc.immo	✓ Noch frei!	3,19 €	Auswählen
dgc.immobilien	✓ Noch frei!	3,19 €	Auswählen



Quelle: hunter.io

DEMO HACK

Vorbereitung



The screenshot shows an email client interface with a dark theme. On the left is a sidebar with navigation icons for 'Schreiben', 'E-Mail', 'Kontakte', and 'Einstellung...'. The main area displays a draft email with the following details:

- Von:** marketing@dgc.email
- An:** olaf.opius@dgc.org
- Betreff:** Sommerfest Umfrage

The email body contains the following German text:

Hallo ihr Lieben,

der Sommer steht vor der Tür, und was gibt es Schöneres als unser jährliches Betriebsfest. Es wird Essen, Getränke und eine Menge Spaß geben!

Damit möglichst viele von euch teilnehmen können, möchten wir eine Abstimmung durchführen, um den perfekten Termin für dieses Fest zu bestimmen.

Deshalb bitte ich euch, die angehängte Exceltabelle auszufüllen.

Vielen Dank für Eure Mithilfe!

Alles Liebe,
Team Marketing

At the bottom left is a blue 'Senden' button. At the bottom right is a link 'In neuem Fenster öffnen'.

On the right side, the 'Optionen und Anhänge' panel is visible. It shows a maximum file size of 10 MB and a button 'Datei anhängen'. Below this, the attached file 'Sommerfest Umfrage.xls (52 KB)' is listed with a download icon. Further down are settings for 'Empfangsbestätigung (MDN)', 'Übermittlungsbestätigung (DSN)', 'Priorität' (set to 'Normal'), and 'Nachricht speichern in' (set to 'Gesendet').

DEMO HACK

Sicht des Opfers



The screenshot shows the Microsoft Outlook interface. The window title is "Suchen". The ribbon includes "Datei", "Start", "Senden/Empfangen", "Ansicht", "Hilfe", and "Nachricht". The "Nachricht" ribbon is active, showing options like "Calibri (Textkör)", "11", "F", "K", "U", "A", and "Laut vorlesen".

The left sidebar shows the "Favoriten" section with "Posteingang", "Gesendete Elemente", and "Entwürfe [1]". Below this, the email account "olaf.opius@dgc.org" is listed with "Posteingang", "Entwürfe [1]", "Gesendete Elemente", "Gelöschte Elemente", "Archiv", "Junk-E-Mail", "Postausgang", "RSS-Feeds", "Verlauf der Unterhaltung", and "Suchordner".

The main area shows a draft email titled "Firewall Audit Notes" with the subject "Moin Hans, ich wollte dich". The "An" and "Cc" fields are empty. The "Betreff" field contains "Firewall Audit Notes". The body of the email contains the text "Moin Hans, ich wollte dich erneut darauf hinweisen, dass wir morgen das Firewall Audit haben und ich noch unbed".

The bottom status bar shows "Elemente: 1", "Alle Ordner sind auf dem neuesten Stand.", "Verbunden mit Microsoft Exchange", and the system tray with "22°C Sonntag", "14:34", and "31.08.2022".

DEMO HACK

Sicht des Angreifers

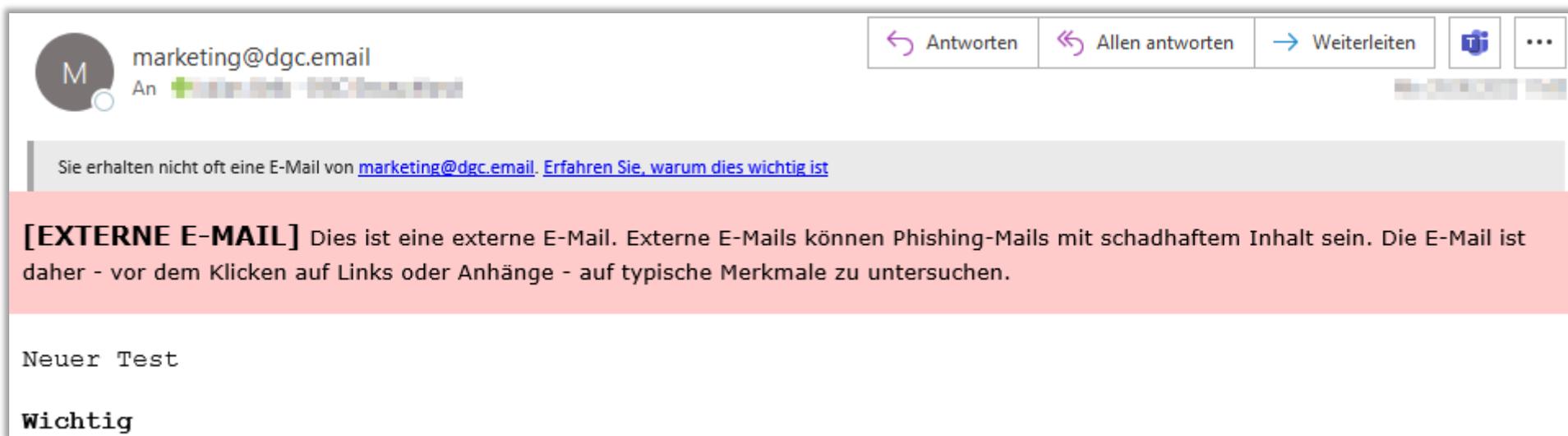
A screenshot of a Metasploit terminal window. The window title is 'msf'. The menu bar includes 'Datei', 'Aktionen', 'Bearbeiten', 'Ansicht', and 'Hilfe'. There are three tabs: 'misc x', 'msf x', and 'web-server x'. The terminal content shows the prompt 'msf6 exploit(multi/handler) >' with a cursor. The background of the terminal is dark blue with a faint grid pattern.

```
msf6 exploit(multi/handler) >
```

DEMO HACK

Zusammenfassung

- Ein gut vorbereiteter Angriff, kann lange unentdeckt bleiben
- Begrenzung und Einschränken des Demo Hacks
- Technische Maßnahmen sind nur die erste Barriere
- Der Mensch selber ist das Hauptziel und muss daher geschult werden



The screenshot shows an email client interface. At the top, there is a header bar with a profile picture of 'M' and the email address 'marketing@dgc.email'. To the right of the header are buttons for 'Antworten', 'Allen antworten', 'Weiterleiten', and a menu icon. Below the header, a warning banner is displayed: 'Sie erhalten nicht oft eine E-Mail von marketing@dgc.email. Erfahren Sie, warum dies wichtig ist'. Below the warning, a red box contains the text: '[EXTERNE E-MAIL] Dies ist eine externe E-Mail. Externe E-Mails können Phishing-Mails mit schadhaftem Inhalt sein. Die E-Mail ist daher - vor dem Klicken auf Links oder Anhänge - auf typische Merkmale zu untersuchen.' Below the red box, the email content begins with 'Neuer Test' and 'Wichtig'.

Q&A

Haben Sie noch Fragen?



KONTAKT

Sprechen Sie uns bei Fragen gerne an!



Auf der Messe

- Halle 7
- Stand 445

Julian Geils

- julian.geils@dgc.org

Vielen Dank für die Aufmerksamkeit!



Tel: +49 461 995 838 0

info@dgc.org
www.dgc.org

Folgen Sie uns in den sozialen Medien, um täglich Beiträge zu den neusten Schwachstellen, Datenpannen und IT- Sicherheitsnews zu erhalten!

