deutsches forschungsnetz

# Neues aus der Phishküche

BT 84 | 17.03.2026

Patrick Welzel

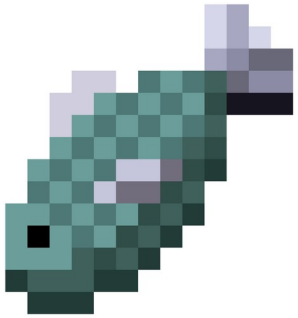
# Motivation

- Mailsupport Workshop November 2025 in Köln
- Phishing beschäftigt alle, gefühlt mehr als Spam
- Schwieriger zu erkennen als Spam
- Oft in Wellen → Geschwindigkeit sehr wichtig!
- KI generiert immer bessere Phishingmails

Wir müssen uns im Mailsupport mehr mit dem Thema beschäftigen

# Derzeitige Maßnahmen

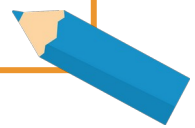
- RBLs von Spamhaus
- Teilweise Virenscanner, vor allem ClamAV
- Manuelle Spamassassin Regeln, vor allem für URIs



# Phish an die Hotline

- Teilnehmende Admins melden Phishing Mails an der Hotline
- An der Hotline werden die Mails manuell angeschaut und **URLs** geblockt
- Blocken geschieht über **Spamassassin** → Braucht Zeit bis auf allen MGWs
- Wenn Hotline ausgelastet → Verarbeitung dauert lange
- Manueller Garbage-Run

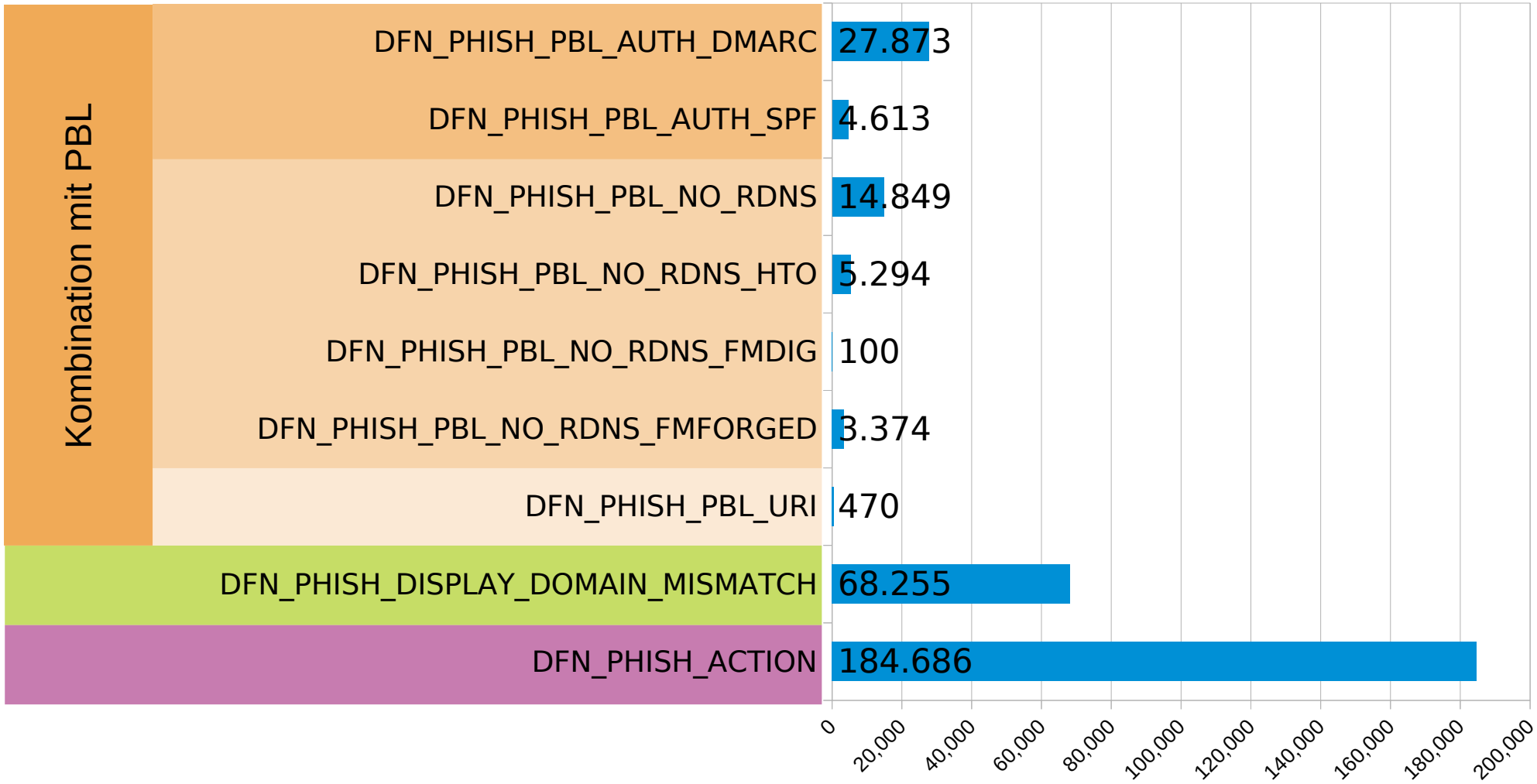
| | |
|---|---|
| Eingetragene Regeln: | ~600 |
| Noch aktive Regeln: | ~90 |



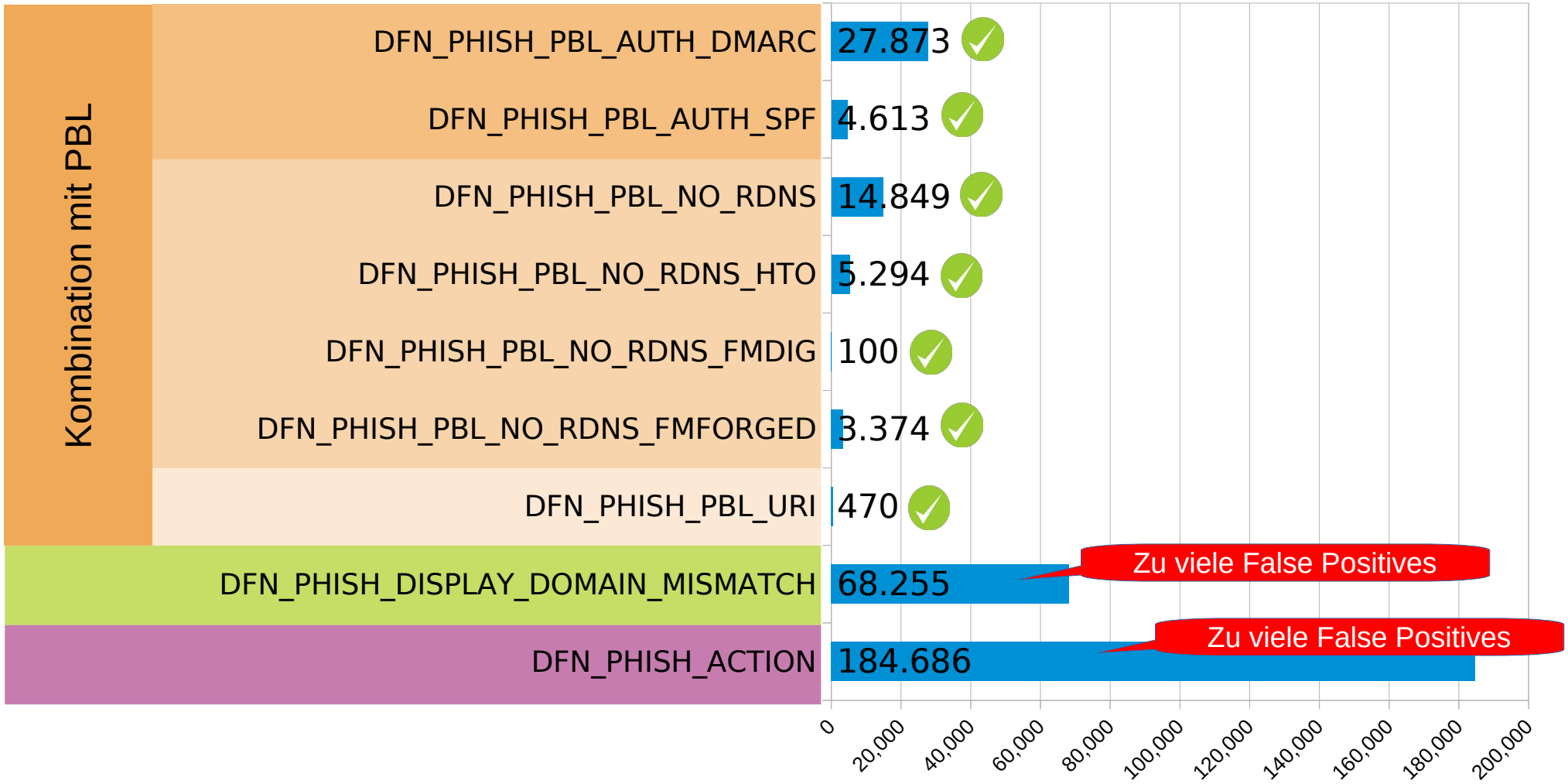
# Neue Maßnahmen – Statische Regeln

- Kombinationsregeln: Spamhaus PBL (Policy Blocklist) +
  - DMARC- / SPF-Fail
  - RDNS_NONE +
    - MIME_HTML_ONLY
    - FREEMAIL_ENVFROM_END_DIGIT
    - FREEMAIL_FORGED_REPLYTO
  - URI_WPADMIN / URI_PHISH
- Display Domain Mismatch
- Phish Action

# Statische Regeln – Statistik über 14 Tage



# Statische Regeln – Statistik über 14 Tage



# Statische Regeln – DMARC Auth

- Die Kombi aus PBL und DMARC zeigt recht gute Ergebnisse
- Wie verbreitet ist denn DMARC bei den Einrichtungen?

| | Anzahl | % |
|---|---|---|
| Mailsupport Domains | 5132 | |
| mit DMARC | 2729 | 53,18% |
| ohne DMARC | 2403 | 46,82% |
| Unterschiedliche Records | 354 | |

# Phishtraining – Neue Trainingsadresse

- Wie so oft: Wir sind auf die Community angewiesen!
- Wir wollen Daten zu Phishing Mails sammeln um…
  - … daraus zu lernen
  - … bessere Regeln zu generieren
  - … schneller reagieren zu können
- Dafür: Eine neue Trainingsadresse neben den bekannten ham, spam, und newsletter Adressen

**phish-TRAINPASSWORD@sXXXY.mx.srv.dfn.de**

# Phishtraining – Was wird analysiert

- URI’s
  - Abgeglichen mit Ignorelists (Mailsupport Domains, DFN Domains, Manuell gepflegt)
  - Gesichert als JSON → Daraus werden **Blocklisten** generiert (für Spamassassin)
- Header
  - Welche Checks haben bereits zugeschlagen? Kann man diese **kombinieren**?
  - Absender Domains, IP’s, etc
  - Können daraus **Muster** und **Regeln** abgeleitet werden?

# Was tun wenn Phish zugestellt wurde?

- Mail mit URI wird gescannt, als unbedenklich eingestuft
- Zustellung, Mail landet beim Nutzer
- Im Nachhinein wird zugestellte URI als Phish erkannt

## Was kann man tun?

1) DNS RPZ vom DFN Cert

2) URL-Rewrite / Save-Links...

# Safe-Links

## NUR EIN GEDANKENSPIEL

- Alle URIs werden auf den MGWs **umgeschrieben**
  - https://urlcheck.mailsupport.dfn.de/?orig=ORIGINAL-URI
- Die Original URI wird **beim Klick** gegen eine Datenbank geprüft
  - Wenn unbedenklich: Weiterleitung
  - Wenn bedenklich: Weiterleitung an **Landing-Page**
- Time-Of-Click anstatt Time-Of-Delivery
- Mehr Zeit für das Prüfen der URI

# Safe-Links – Pro & Contra

| | |
|---|---|
| **PRO** | Time-Of-Click anstatt Time-Of-Delivery |
| **PRO** | Mehr Zeit für das Prüfen der URI |
| **PRO** | Nachträglicher Schutz |
| **CONTRA** | Hoher Aufwand (Rewrite, Landingpage, Datenbank, …) |
| **CONTRA** | Eingriff in den Mailinhalt |

# Danke für die Aufmerksamkeit!

Gibt es Fragen?