deutsches forschungsnetz

"Werkzeuge für die Spam- und Phishing-Erkennung beim DFN-MailSupport"

79. DFN-Betriebstagung | Forum Mail | 17.10.2023

Andrea Wardzichowski DFN-Verein

Spam-Erkennung (1)

Checks

Folgende Checks werden von den Gateways in dieser Reihenfolge durchgeführt. Einzelne Checks können auf Wunsch modifiziert oder auch abgeschaltet werden. Die Checkgruppe entscheidet darüber, welche Aktionen auf eine Mail angewendet werden können.

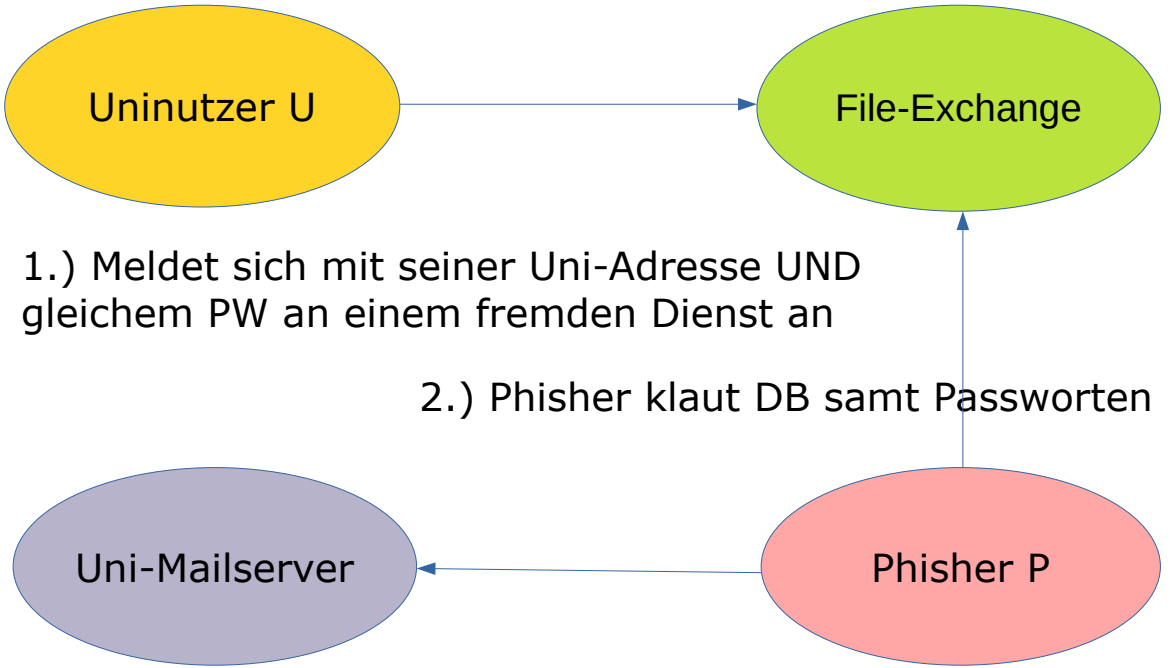
Check	Checkgruppe	Beschreibung
dynamische Blacklisten	kernel	Lastreduktion bei Botnetz-Attacken
Verhalten	postfix-smtpd	SMTP-Protokoll-Konformität
RBL	postfix-smtpd	Reputation des einliefernden Mailhosts
Black-/Whitelists	postfix-smtpd	Konfigurierbare Black- und Whitelisten
DNS	postfix-smtpd	Maildomain des Absenders sowie DANE
SPF	postfix-smtpd oder wahlweise amavis-spam	Kontrolle der Kombination von Envelope-Absenderadresse und einlieferndem Mailserver
User Verify	postfix-smtpd	Existiert die Adresse auf dem Zielmailserver der Einrichtung?
Größe	postfix-smtpd	Größe der Mail
Ratelimiting	postfix-smtpd	Limitierung ausgehender Mails
Anhänge	amavis-banned, amavis-unchecked	Unerwünschte Attachment-Typen bzw -Namen
Header	postfix-cleanup, amavis-dkim	Inhalt der Mail-Header
Viren	amavis-virus	Viren erkennen
DKIM	amavis-spam	DKIM-Signaturen validieren
DMARC	amavis-spam	Header-From validieren
ARC	amavis-spam	Weiterleitungs-Signaturen validieren
URL	amavis-spam	URLs in Emails erkennen und bewerten
Spam	amavis-spam	Spam erkennen

Spam-Erkennung (2)

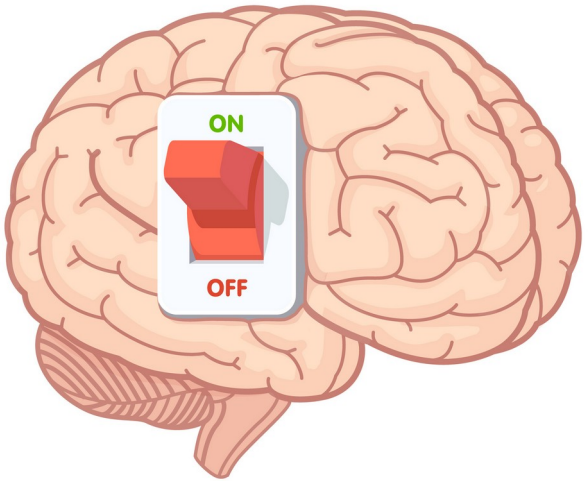
- Automatisiert erkennbar
- Viel: Mustererkennung
- Aufaddieren von Spam-Punkten pro Check
- Inhalt: Bayesfilter mit statistischer Wortgewichtung
- X-Spam-Score, einfaches Wegsortieren möglich

=> Manche Dinge können Rechner besser als Menschen

Warum sehen Phishing-Mails nicht wie Spam aus?



Phishing-Erkennung (1)



Quelle: freepik.com, Author: iconicbestiary

Phishing-Erkennung (2)

- Kann nur durch eine Person erkannt werden
- z.B. anhand einer „komischen“ Absenderadresse
  => IMMER die ganze Mailadresse anzeigen lassen,
  nicht nur den „real name“ Teil!
- Oder verdächtigen Inhalten
- Oder an verdächtigen Links, wenn man mit der Maus über die Links geht, ohne zu klicken
  => die URL, die angezeigt wird, muß nicht die sein, auf die man durch Klicken dann geleitet wird.

Phishing-Erkennung (3)

- Auf „Umwegen“
  - URLs aus Phishingmails werden uns aus der Community gemeldet und in eine Blacklist eingetragen
  - Diese Blacklist muß aber in regelmäßigen Abständen bereinigt/gekürzt werden
  - Oft ist die Phishingwelle schon vorbei, wenn die URL bei uns ankommt
  - Einträge nur wochentags zu Bürozeiten.

DNS-Blocklisten des SWITCH

- DNS-RPZ „Domain Name System Response Policy Zone“
- Prüft den Host-Teil der URL gegen eine Blocklist im DNS
- Einbindung in den Resolver-DNS der Einrichtung
- Verhindert nicht, dass die Mail ins Postfach zugestellt wird, aber immerhin, dass die Schad-URL aufgerufen wird!

- DFN-MailSupport plant: Einbindung der Blocklisten und Check der URL gegen diese Listen per DNS
- Addieren von Spampunkten (in der Folge Ablehnung oder Markierung als Spam)

Kontakt

WWW: https://www.mailsupport.dfn.de/
Mail: hotline@mailsupport.dfn.de
Tel.: +49 711 / 633 14 217

Vielen Dank für die Aufmerksamkeit!