TECHNISCHES WHITEPAPER · VORGESCHLAGENES RAHMENKONZEPT · VERSION 1.0

Von der Erkennung zur Umsetzung

Eine messbare Architektur für die Reaktion auf DNS Abuse: Provenienz der Beweismittel, verhältnismäßige Maßnahmen, öffentliche Rechenschaftspflicht und schnelle Einsprüche – konzipiert für empirische Erprobung statt bloßer Behauptung.

- Veröffentlicht am 2. August 2026
- PhishDestroy Forschung
- Entwurf zur öffentlichen Konsultation
- Nicht begutachtet

PD-WP-2026-01 · Version 1.0 · 2026-08-02
https://phishdestroy.io/de/dns-abuse-enforcement-framework

ZUSAMMENFASSUNG

EIGENSTÄNDIGER VORSCHLAG · KEIN ICANN-PROGRAMM

Direkte Schlussfolgerung. Das vertragliche Ökosystem von „gTLD“ weist eine messbare Lücke zwischen der technisch nachgewiesenen missbräuchlichen Nutzung einer Domain und wirksamen Abhilfemaßnahmen auf. Veröffentlichte Studien zeigen, dass viele Phishing-Kampagnen stunden- oder tagelang laufen, während Verfahren zur Einhaltung vertraglicher Verpflichtungen sich über mehrere Werktage erstrecken können. Das dargestellte Szenariomodell veranschaulicht, wie Verzögerungen die erwarteten Erträge der Kampagnen erhöhen; der Bereich von 60–85 % ist die zentrale, überprüfbare Schätzung des in der Studie beschriebenen Schadens nach Bekanntgabe und keine feststehende Statistik für den gesamten weltweiten Betrug. Die technische Schätzung von 100–150 US-Dollar bezieht sich auf die Erfassung und Erstverarbeitung eines definierten Korpus aus Zonen-, Certificate-Transparency- und Public-Feed-Daten, nicht auf die Gesamtkosten einer rechtlichen Prüfung oder Durchsetzung. Die Studie schlägt signierte Nachweise, messbare Reaktionsziele, die automatische Eskalation validierter Fälle, verhältnismäßige Abhilfemaßnahmen, öffentliche Rechenschaftspflicht und ein zügiges Berufungsverfahren vor. Sie schlägt nicht vor, Meldenden direkten Zugriff auf die Steuerungsmechanismen zur Domainsperrung zu gewähren.

PRIMÄRQUELLE
Durch ein offizielles Dokument oder eine veröffentlichte Studie direkt belegt.

VERANSCHAULICHENDES MODELL
Eine reproduzierbare Berechnung, deren Eingabewerte auf Annahmen und nicht auf Marktdurchschnittswerten basieren.

VORSCHLAG FÜR EINE GOVERNANCE-REGELUNG
Ein Entwurf zur Konsultation, Erprobung und Überarbeitung.

01 Forschungsfrage, Umfang und Beweisstandard

Die Frage ist enger gefasst als „Wer hat versagt?“: **Welche erkennbaren Verzögerungen zwischen validierten Beweisen und angemessenen Maßnahmen lassen sich vermeiden, und welche Maßnahme mindert den Schaden für die Opfer, ohne dass dabei inakzeptable Fehlalarme oder Kollateralschäden entstehen?**

Der Geltungsbereich umfasst das vertraglich festgelegte gTLD-Ökosystem: Registranten, Wiederverkäufer, Registrare, Registries und die für die Vertragskonformität zuständige Stelle von ICANN. Hosting-Anbieter, CDNs, Browser, Zahlungsdienste, Werbeplattformen, nationale CERTs und Strafverfolgungsbehörden werden nur dann einbezogen, wenn sie die Beweiskette oder die Reaktionskette beeinflussen. Ländercode-TLDs unterliegen einer anderen Governance und gelten nicht als Gegenstand der „gTLD“-Verträge von ICANN.

Stand der zentralen Thesen

- Der Beitrag analysiert „ICANN“ als private Institution zur Governance und zur Durchsetzung vertraglicher Verpflichtungen innerhalb des Ökosystems „gTLD“. „ICANN“ ist keine staatliche Regulierungs- oder Strafverfolgungsbehörde, akkreditiert jedoch Registrare, schließt Verträge mit Registrierungsbetreibern ab und sorgt für die Einhaltung dieser Vereinbarungen; dieser begrenzte Aufgabenbereich entbindet die Institution nicht von ihrer Rechenschaftspflicht.
- Der Bereich von 60–85 % ist eine zentrale quantitative Schätzung im Schadensmodell der Studie. Er wird als überprüfbare Schätzung dargestellt, die sich aus expliziten Annahmen und Fallbeobachtungen ableitet – nicht als bereits feststehende Statistik für den gesamten weltweiten Betrug. Die Veröffentlichung eines Datensatzes auf Vorfallsebene, der die Zeitstempel für Erkennung, Benachrichtigung, Schadensbegrenzung und Schaden miteinander abgleicht, ist der nächste Schritt zur Belegung der Ergebnisse.
- Der Betrag von 100–150 US-Dollar ist eine überprüfbare technische Kostenschätzung für die kontinuierliche Erfassung und erste Triage anhand eines definierten Satzes von Daten zu zugänglichen Zonen, „Certificate Transparency“ und öffentlichen Feeds auf Standardinfrastruktur. Es handelt sich dabei nicht um die Kosten für vollständige globale Transparenz, rechtliche Prüfung, Einsprüche, Hochverfügbarkeit oder Durchsetzung. Das Papier behandelt diesen Wert daher als Richtwert, der anhand einer veröffentlichten Arbeitslast, eines Quellenverzeichnisses und eines Kostenprotokolls reproduziert werden kann – nicht als bereits bewährten universellen Preis. Diese Unterscheidung schränkt die Aussage ein, ohne die getestete Kostenasymmetrie auszublenden.
- Der in der Studie durchgeführte dreiwöchige Vergleich bezieht sich auf die Latenz bei der Einhaltung der Vorschriften und nicht auf eine allgemeine SLA für die Sperrung von Domains. ICANN’s Häufig gestellte Fragen zur Vertragseinhaltung Darin heißt es, dass die meisten Beschwerdearten drei aufeinanderfolgende Antwortfristen von jeweils fünf Werktagen durchlaufen können, bevor eine formelle Eskalation erfolgt, während viele böswillige Kampagnen über Stunden oder Tage hinweg andauern. In den Verträgen ist gesondert festgelegt, dass nach Vorliegen verwertbarer Beweise unverzüglich angemessene Abhilfemaßnahmen zu ergreifen sind. [2] [4]
- Im Falle einer nachweislich böswilligen Registrierung, die ausschließlich einem bestimmten Zweck dient, `serverHold` Gehört zu den Maßnahmen auf DNS-Ebene mit den größten Auswirkungen, da dadurch die Delegierung aus der Zone entfernt wird. Die Maßnahme ist nicht universell anwendbar: Sie kann auch den E-Mail-Verkehr, Subdomains und legitime Dienste beeinträchtigen; zwischengespeicherte Antworten können bis zum Ablauf der TTL bestehen bleiben; und bei kompromittierten oder gemeinsam genutzten Diensten sind unter Umständen gezieltere Abhilfemaßnahmen erforderlich. [4] [7]

FORSCHUNGSBEITRAG

Der Vorschlag ist falsifizierbar. Ein Pilotversuch kann Behandlungs- und Kontrollkohorten anhand der Zeit bis zur Triage, der Zeit bis zur Risikominderung, der Indikatoren für Opferverluste, der Wiederholungsrate, der Falsch-Positiv-Rate, der Aufhebungszeit und der Kollateralauswirkungen vergleichen.

02 Was die Primärquellen belegen

$165.1M

ICANN-Betriebsfinanzierung im Geschäftsjahr 2027

Verabschiedeter Haushalt für das Geschäftsjahr 2027. Kontextuelle Größenordnung; keine Angabe zu Ausgaben für DNS Abuse. [1]

191,561

Beschwerden wegen Phishing/Spoofing im Jahr 2025 (IC3)

Größte IC3-Beschwerdekategorie nach Anzahl; direkt zugeordnete Verluste in Höhe von 215,8 Mio. $. [10]

24 Std.

Mediane Lebensdauer in einer Studie aus dem Jahr 2021

Datensatzspezifisches Ergebnis für 1.288 Phishing-Domains; keine allgemeingültige Lebensdauer. [11]

Kein festes SLA

Allgemeingültige Abschaltfrist

Die Änderungen von 2024 verlangen „unverzügliche“ und „angemessene“ Risikominderung, nicht eine einzige globale Frist. [2] [3]

THESE	STATUS	WAS LÄSST SICH SAGEN?
Phishing ist DNS Abuse	VERIFIZIERT	Phishing ist ausdrücklich eine der fünf Kategorien der gTLD-Vertragsänderungen von 2024. [2]
Registrare müssen handeln	VERIFIZIERT	Registrare müssen unverzüglich handeln, wenn ihnen verwertbare Beweismittel dafür vorliegen, dass ein von ihnen betreuter Domainname für DNS Abuse genutzt wird. [2]
Registry-Betreiber müssen handeln	VERIFIZIERT	Registry-Betreiber müssen unverzüglich handeln, wenn sie auf Grundlage verwertbarer Beweismittel nach vernünftigem Ermessen feststellen, dass ein registrierter Domainname für DNS Abuse genutzt wird; die angemessene Maßnahme bleibt kontextabhängig. [3]
`serverHold` entfernt die Delegierung	VERIFIZIERT	Es handelt sich um einen serverseitig gesetzten EPP-Status. Zwischengespeicherte DNS-Antworten können bis zu ihrem Ablauf fortbestehen; die Maßnahme betrifft die gesamte registrierte Domain. [7]
Jeder Fall von DNS Abuse ist in CZDS oder CT sichtbar	FALSCH	CZDS und Certificate Transparency sind wertvolle Sensoren, bieten aber weder einen vollständigen noch einen durchgehend echtzeitnahen Überblick über jede Domain-Nutzung. [8] [9]

Der erste Halbjahresbericht der ICANN zur Umsetzung der Änderungen von 2024 verzeichnete 192 Untersuchungen, mehr als 2.700 gesperrte Domains, mehr als 350 deaktivierte Phishing-Seiten und zwei formelle Vertragsverletzungsanzeigen (Notices of Breach). Diese Zahlen belegen nicht, dass die heutigen Kontrollen ausreichen; sie widerlegen jedoch die pauschale Behauptung völliger Untätigkeit. [5]

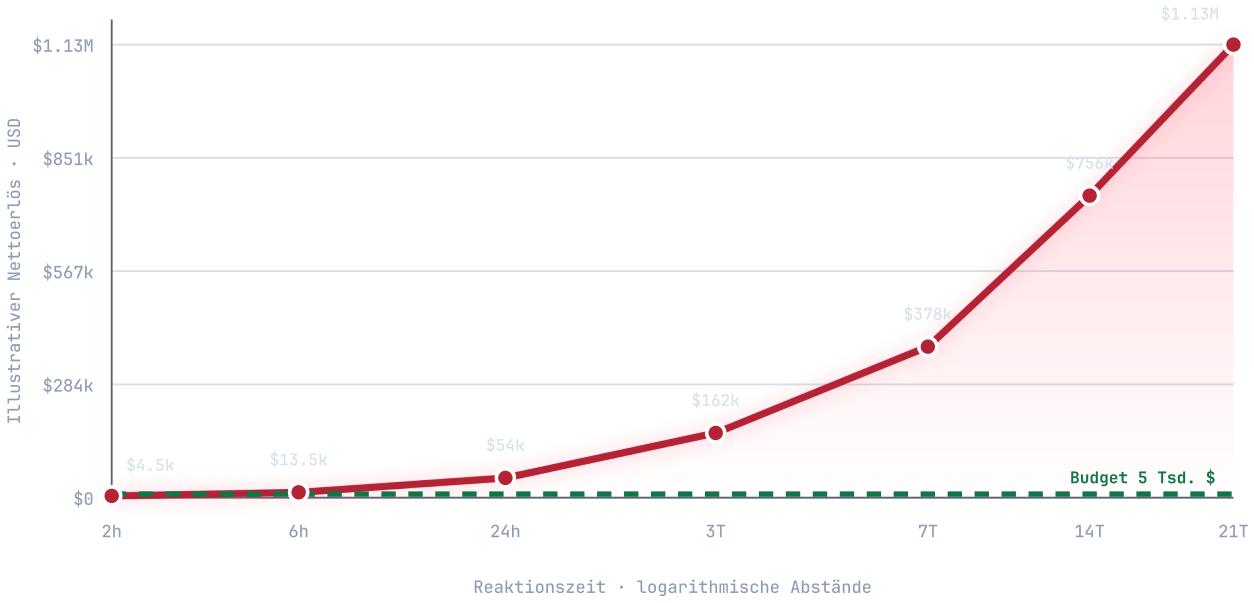
03 Warum die Antwortlatenz nach wie vor ein berechtigtes Forschungsziel ist

Manche Phishing-Kampagnen laufen über einen Zeitraum von Stunden oder Tagen. Bijmans et al. berichteten in einer Studie aus dem Jahr 2021 über eine durchschnittliche beobachtete Lebensdauer von 45 Stunden und einen Median von 24 Stunden für 1.288 Phishing-Domains. Eine Studie aus dem Jahr 2026 über neu registrierte Phishing-Domains ergab eine stark schiefe Verteilung: Bei 14.112 Domains mit messbarer Lebensdauer betrug der Mittelwert 8,6 Tage und der Median einen Tag. Keine der beiden Stichproben lässt sich auf alle Bedrohungsklassen verallgemeinern, doch beide zeigen, warum ein Prozess, der nur in Werktagen gemessen wird, kurzlebige Kampagnen übersehen kann. [11] [12]

> **DIE GEMESSENE ZEITLICHE DISKREPANZ**
>
> Diese Studien ermitteln zwar nicht den Anteil des finanziellen Schadens, der nach der Benachrichtigung entsteht, belegen jedoch eine zeitliche Diskrepanz: Ein Prozess, dessen frühe Phasen der informellen Einhaltung bis zu fünfzehn Werktage in Anspruch nehmen können, kann für Kampagnen mit einer medianen Laufzeit von etwa einem Tag allein nicht als Incident Response dienen. Der unten angeführte 21-Tage-Zeitpunkt stellt daher ein Szenario mit Compliance-Latenz dar und ist keine Bezeichnung für ein universelles „ICANN-SLA“.

ABBILDUNG 1 · VERANSCHAULICHUNG DES KUMULATIVEN KAMPAGNENERGEBNISSES

MODELL · LOGARITHMISCHE ZEITABSTÄNDE



Die Kurve veranschaulicht das in Abschnitt 4 beschriebene Szenario; es handelt sich nicht um beobachtete Marktdaten. Durch die horizontale Darstellung werden lange Zeitintervalle zur besseren Lesbarkeit komprimiert. Quelle: reproduzierbares Modell mit offengelegten Eingabewerten.

VORSICHT BEI DER KAUSALITÄTSZUORDNUNG

Eine kürzere Lebensdauer einer Domain bedeutet nicht automatisch, dass finanzielle Verluste verhindert werden. Angreifer können ihre Aktivitäten verlagern, kompromittierte Websites nutzen, ihre Verbreitungskanäle ändern oder ihre Gewinne vor der Entdeckung auszahlen lassen. Der kausale Zusammenhang muss gemessen werden und darf nicht allein aus der Geschwindigkeit der Abschaltung abgeleitet werden.

04 Ökonomie von Betrugskampagnen als reproduzierbares Szenario

Der wirtschaftlich relevante Wert liegt häufig nicht in der Registrierungsgebühr, sondern in Traffic, Werbemitteln, Infrastruktur und Vertrauen, die sich um eine Domain herum aufgebaut haben. Diese Annahme ist plausibel; ihre Größenordnung variiert je nach Betrugskampagne. Der folgende Rechner legt daher sämtliche Eingaben offen, statt ein hypothetisches Ergebnis als beobachteten Durchschnitt auszugeben.

MODELLDEFINITION

```
visits(T)   = daily_traffic × T / 24
victims(T)  = visits(T) × conversion_rate
proceeds(T) = victims(T) × average_loss × (1 - cashout_attrition)
profit(T)   = proceeds(T) - campaign_budget
```

Szenario-Rechner

Ändern Sie eine beliebige Annahme. Die Werte dienen lediglich der Veranschaulichung und stellen keine Schätzungen des typischen Phishing-Marktes dar.

VERANSCHAULICHENDES MODELL

Kampagnenbudget (USD)

5000

Tägliche Besuche

2000

Konversionsrate der Opfer (%)

1.5

Durchschnittlicher Schaden pro Opfer (USD)

2400

Verlustquote beim Cash-out (%)

25

Dauer der Maßnahme (Stunden)

24

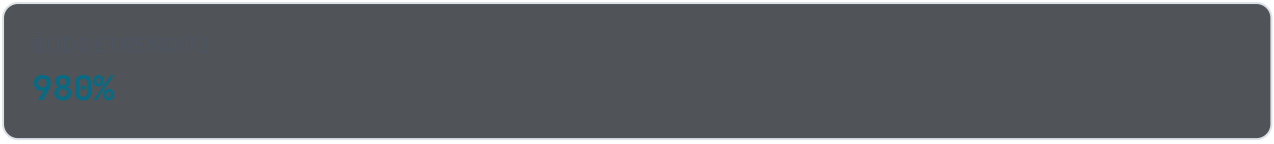
Besuche
2,000

Konversionen pro Tag
30

Tagesschaden
$54,000

Gesamtschaden
$49,000

Amortisationszeit
2.2 h



Die erwartete Opferzahl kann Dezimalstellen enthalten, weil das Modell einen Erwartungswert ausgibt. Nicht berücksichtigt werden rückläufiger Traffic, Rückkopplungen durch die Erkennung, Migration, wiederholt betroffene Opfer und Unsicherheitsverteilungen.

▶ Modellquelltabelle anzeigen

05 Vermeidbare Schäden messen, ohne Präzision zu erfinden

„Verlust nach Aufdeckung“ kann nur dann als nützliches Ergebnis gewertet werden, wenn die Begriffe „Aufdeckung“, „Übermittlung“ und „Schaden“ einheitlich definiert sind. Ein Zeitstempel auf einer schwarzen Liste ist kein Beweis dafür, dass der Registrar verwertbare Beweise erhalten hat. Eine Wallet-Transaktion lässt sich nicht automatisch einer bestimmten Domain zuordnen. Die Tatsache, dass eine Domain nicht mehr erreichbar ist, gibt keinen Aufschluss darüber, welcher Akteur diese Änderung verursacht hat.

Mindestschema für Ereignisse

EREIGNIS	ERFORDERLICHER ZEITSTEMPEL	MINDESTNACHWEIS
Erste Beobachtung	`t_obs`	Sensor, Hashwert für Anfrage/Antwort, Erfassungsmethode, Taktquelle.
Technische Validierung	`t_valid`	Reproduzierbarer Indikator, Identität des Gutachters, Bedrohungskategorie und Konfidenz.
Benachrichtigung zugestellt	`t_notice`	Authentifizierte Zustellbestätigung und Version des Evidence Envelope.
Verantwortlicher Akteur bestätigt den Eingang	`t_ack`	Fall-ID und Zielrolle: Host, Registrar, Registry, Plattform oder Behörde.
Risikominderung beobachtet	`t_mitigate`	DNS-, HTTP-, Zahlungs- oder Plattformstatus, gemessen von mehreren Beobachtungspunkten.
Einspruch / Wiederherstellung	`t_restore`	Entscheidungsgrundlage, geänderte Beweislage und Verifikation der Wiederherstellung.
Schadensereignis	`t_harm`	Anonymisierter Opferbericht, zuordenbare Transaktion oder ein anderer dokumentierter Ersatzwert.

VORGESCHLAGENE ERGEBNISKENNZAHL

$$\text{Post-notice harm share} = \frac{\text{attributable harm with } t_{harm} > t_{notice}}{\text{all attributable harm in the observation window}}$$

Für Zähler und Nenner muss dieselbe Zuordnungsregel gelten. In den Ergebnissen sollten die Kohorte, das Konfidenzintervall, die Rechtszensierung, fehlende Quellen, der Umgang mit doppelten Opfern sowie die Sensitivität gegenüber dem Beobachtungszeitraum angegeben werden. Die Bezeichnung „vermeidbar“ sollte einem kausalen Design oder zumindest einem gepaarten Vergleich vorbehalten bleiben – und nicht jedem Ereignis nach Bekanntgabe.

ZENTRALE MODELLSCHÄTZUNG · 60–85 %

Die Studie behält 60–85 % als zentralen Schätzwert für den Anteil des zurechenbaren Schadens bei, der nach der Aufdeckung und Benachrichtigung in der modellierten Vorfallsklasse entsteht. Es handelt sich um eine Szenario-Schätzung, die aus offengelegten Annahmen und Fallbeobachtungen abgeleitet wurde – nicht um eine gemessene Statistik für alle Betrugsfälle weltweit. Sie sollte für Sensitivitätsanalysen herangezogen werden, bis ein Datensatz auf Vorfallsebene die Zeitstempel von Beobachtung, validierten Beweisen, Übermittlung, Schadensminderung und Schaden in Einklang bringt. Die Veröffentlichung dieses Datensatzes ist der Beweis für die These, nicht ein Grund, die These zu verwerfen.

06 Das institutionelle Modell: Die Kompetenzen sind verteilt

Kein einzelner Akteur hat den vollständigen Überblick über den Vorfall oder die Kontrolle darüber. Der Registrar kennt die Beziehung zum Registranten; die Registry kontrolliert den von ihr festgelegten Domainstatus; der Host und der CDN steuern die Bereitstellung von Inhalten; Browser und Sicherheitsanbieter steuern Warnmeldungen; Zahlungs- und Wallet-Anbieter können Übertragungen unterbrechen; Behörden können die Aufbewahrung oder Beschlagnahme anordnen. ICANN erstellt und setzt Verträge im gTLD-Ökosystem durch, betreibt jedoch keine universelle EPP-Steuerungsebene.

01 · SIGNAL

Forschende & Sensoren

Indikatoren zu Inhalten, Infrastruktur und Opfern erfassen; ihre Provenienz bewahren.

02 · SERVICE

Host / CDN / Plattform

Kann Inhalte entfernen oder den Zugriff rasch sperren, häufig ohne die Domain zu verändern.

03 · SPONSOR

Registrar

Überprüft Missbrauchsfälle, kontaktiert den Registranten und kann den Status auf Client-Seite festlegen.

04 · ZONE

Registry-Betreiber

Steuert den registryseitigen EPP-Status und die Delegierung der TLD-Zone.

05 · VERTRAG

ICANN Contractual Compliance

Untersucht die Vertragseinhaltung der gebundenen Parteien; entscheidet nicht über jeden einzelnen Betrugsfall.

06 · RECHT

CERT / Behörden

Koordinieren die Reaktion und nutzen die jeweils zuständigen rechtlichen Befugnisse.

Verteilte Zuständigkeiten bedeuten nicht, dass die Verantwortung entfällt. Ein sponsernder Registrar entbindet sich nicht von seinen vertraglichen Pflichten, indem er die Bearbeitung von Missbrauchsfällen an einen Wiederverkäufer delegiert; die Registry kontrolliert den EPP-Status der Server; ICANN sorgt für die Einhaltung der vertraglichen Verpflichtungen. Der Prüfpfad muss nicht nur festhalten, wer gehandelt hat, sondern auch, wer verwertbare Beweise erhalten, den Fall weitergeleitet, nicht reagiert oder eine zugewiesene Pflicht nicht erfüllt hat. Die rechtliche Befugnis verbleibt bei dem Akteur, der zur Anwendung einer Maßnahme befugt ist; die Rechenschaftspflicht erstreckt sich auch auf dokumentierte Pflichtverletzungen.

Konzentration der Fördermittel und eine überprüfbare Hypothese zu Anreizkonflikten

$165.1M

Finanzmittel für den Betrieb des „ICANN“ im Haushaltsjahr 27

Das Basis-Budget für das Geschäftsjahr 27 wurde verabschiedet. [1]

≈98.1%

Einnahmequellen aus Registrierungs- und Registrierungsstellengebühren

Etwa 162,0 Mio. US-Dollar des Finanzierungsplans in Höhe von 165,1 Mio. US-Dollar. [1]

70.7%

allein transaktionsabhängige Gebühren

$116.8M tied to billable domain transactions. [1]

Die Finanzierungsstruktur stützt sich daher in hohem Maße auf Zahlungen der Vertragspartner, deren Vereinbarungen von ICANN durchgesetzt werden, und ein großer Teil davon hängt von den abrechnungsfähigen Registrierungsvorgängen ab. Dies führt zu einer strukturellen Abhängigkeit und wirft die berechtigte Frage nach einem Anreizkonflikt auf. Dies ist der Fall *nicht*... allein schon als Beweis für eine absichtliche mangelnde Durchsetzung oder eine vollendete „regulatorische Vereinnahmung“ herangezogen werden. Die Hypothese der Vereinnahmung sollte anhand der Reaktionszeiten auf Einzelfallebene, der Ergebnisse der Durchsetzung, der Sanktionen, wiederholter Missbräuche sowie der Rolle finanzierter Interessengruppen bei politischen und umsetzungsbezogenen Entscheidungen überprüft werden.

07 Die vertragliche Ausgangsbasis für 2024 – und was darin nicht festgelegt ist

Die globalen Änderungen vom April 2024 am Registrar Accreditation Agreement und am Base Registry Agreement begründeten ausdrückliche Pflichten zur Eindämmung von DNS Abuse. Registrare müssen unverzüglich handeln, wenn ihnen verwertbare Beweismittel dafür vorliegen, dass ein von ihnen betreuter Domainname für DNS Abuse genutzt wird. Registry-Betreiber müssen unverzüglich handeln, wenn sie auf Grundlage verwertbarer Beweismittel nach vernünftigem Ermessen feststellen, dass ein registrierter Domainname für DNS Abuse genutzt wird. In beiden Fällen hängt die angemessene Maßnahme von Kontext, Schweregrad und Kollateralauswirkungen ab. [2] [3]

Drei Zeitachsen, die oft miteinander verwechselt werden

ZEITLEISTE	WOFÜR DIES GILT	WAS ES NICHT BEDEUTET
24 Stunden	Prüfung nach RAA §3.18.3 von begründeten Berichten über rechtswidrige Aktivitäten („Illegal Activity"), die Strafverfolgungs-, Verbraucherschutz-, quasi-staatliche oder vergleichbare Behörden an den dafür vorgesehenen Kontakt übermitteln.	Es handelt sich nicht um eine allgemeingültige 24-Stunden-Frist für die Sperrung.
„Unverzüglich"	Ergreifen einer angemessenen Risikominderungsmaßnahme, nachdem der jeweils geltende Schwellenwert für verwertbare Beweismittel erreicht ist.	Es handelt sich weder um eine feste Stundenzahl noch ist in jedem Fall dieselbe Abhilfemaßnahme vorgeschrieben.
21 Tage	Kann nach einer formellen vertraglichen Vertragsverletzungsmitteilung als Nachbesserungsfrist gelten.	Es handelt sich nicht um die übliche Lebensdauer, die jeder gemeldeten bösartigen Domain zugewiesen wird.

Diese Flexibilität hat Vorteile: Eine kompromittierte Universitätsdomain sollte nicht wie eine neu registrierte, ausschließlich für Phishing-Zwecke genutzte Domain behandelt werden. Das Problem bei der Rechenschaftspflicht besteht darin, dass sich „unverzüglich" und „angemessen" ohne veröffentlichte Zeitstempel, Fallkategorien und Ergebniscodes nur schwer miteinander vergleichen lassen. Der nachstehende Vorschlag sieht Mess- und Überprüfungsmechanismen vor, ohne dabei so zu tun, als gäbe es eine einheitliche Frist, die für alle Fälle gilt.

08 Das Abgrenzungsproblem: Phishing wird abgedeckt; bestimmte Formen des Finanzbetrugs möglicherweise nicht

Phishing fällt ausdrücklich unter die vertragliche Definition von DNS Abuse. Schwieriger abzugrenzen sind Websites, die Nutzer unter einem eigenen Namen täuschen, statt sich als identifizierbarer Dritter auszugeben: etwa bestimmte fingierte Anlageplattformen, betrügerische Shops, Recovery Scams und Systeme zum Erschleichen von Wallet-Signaturen. Je nach Sachverhalt können diese als Missbrauch

von Website-Inhalten, Verbraucherbetrug oder eine andere Rechtskategorie und nicht als vertraglicher DNS Abuse behandelt werden.

> VORGESCHLAGENER FORSCHUNGSBEGRIFF
>
> **Verified Financial Harm Abuse (VFHA)**: dokumentierte Nutzung einer Domain, um durch Täuschung Geldmittel, Zahlungsdaten, private Schlüssel oder Seed-Phrasen zu erlangen, unabhängig von einer Markenimitation. VFHA ist kein Begriff der geltenden ICANN-Terminologie und begründet für sich genommen keine vertragliche Befugnis.

Eine politische Konsultation könnte prüfen, ob eine eng abgegrenzte, evidenzgestützte Kategorie wie VFHA in künftige Verträge, einen sektorübergreifenden Verweisungsrahmen oder nationales Recht gehört. Jede Erweiterung sollte eine präzise Schadensprüfung, belastbare Beweismittel, verhältnismäßige Abhilfen, eine Prüfung der Zuständigkeit und einen Einspruchsweg voraussetzen. Pauschale Bezeichnungen wie „Scam“ reichen nicht aus.

09 Was die Behauptung bezüglich der Überwachungskosten von 100–150 Dollar pro Monat beweisen muss – und was sie nicht beweisen kann

Ein Standard-Server kann öffentlich zugängliche Snapshots der an „gTLD“ teilnehmenden Zonendateien herunterladen und Änderungen lokal berechnen, ausgewählte „Certificate Transparency“-Ereignisse und offene Feeds erfassen, Zeichenfolgen normalisieren, Hashes berechnen und Kandidaten priorisieren. Das ist ein nützlicher, testbarer technischer Maßstab – keine „vollständige Überwachung des Internets“. Im zweiten Quartal 2026 meldete Verisign 401,6 Millionen Registrierungen über alle TLDs hinweg; CZDS deckt teilnehmende „gTLD“-Zonendateien ab und nicht alle TLDs, und CT erfasst öffentlich protokollierte Zertifikate oder Vorzertifikate und nicht jede aktive oder schädliche Domain. [8] [9] [17]

FÄHIGKEIT	PROTOTYP AUF STANDARDHARDWARE	PRODUKTIVDIENST IM ÖFFENTLICHEN INTERESSE
Zonen-/CT-/Feed-Erfassung	Für eine definierte Quellengruppe machbar	Redundante Kollektoren, Lieferverträge und Lückenüberwachung
String-/Hash-Triage	Machbar	Benchmarking, Drift-Erkennung, Untersuchungen zu falsch-negativen Ergebnissen
Browser-Rendering	Kleine Stichprobe	Isolierte Flotte, regionale Beobachtungspunkte, Eindämmung von Malware
Rechtliche Feststellung	Nicht enthalten	Qualifizierte Prüfer, Zuständigkeit und Zuordnung von Befugnissen
Hohe Verfügbarkeit / Aufbewahrung von Beweismitteln	In der Regel nicht vorhanden	HSM-gestützte Signaturen, Prüfprotokolle, Backups und Reaktion auf Sicherheitsvorfälle
Rechtsmittel und Wiedereinsetzung	Nicht enthalten	Betrieb rund um die Uhr, eigenständige Eskalation und Serviceziele

ABBILDUNG 2 · GRÖSSENORDNUNGSZUSAMMENHANG LOGARITHMISCHE BREITE · NICHT VERGLEICHBARE KOSTEN

Logarithmische Breiten sorgen dafür, dass kleine Werte sichtbar bleiben. Bei den ersten drei Zahlen handelt es sich um offengelegte technische oder programmatische Annahmen, die einen veröffentlichten Referenzwert erfordern, und nicht um Angebote von Anbietern. ICANN Die Betriebsfinanzierung ist eine verifizierte Zahl im institutionellen Maßstab. Es handelt sich hierbei bewusst um nicht vergleichbare Budgets: Der Vergleich dient dazu zu prüfen, ob die grundlegende Datenerfassung und Triage an sich schon unerschwingliche Kosten verursachen, und nicht, ob ein vollständiges Durchsetzungsprogramm 100 Dollar pro Monat kostet.

10

Vorgeschlagenes Verified Abuse Response Framework

Der vorgeschlagene Rahmen ist eine Referenzarchitektur, kein automatischer globaler „Kill Switch“. Er standardisiert den Evidence Envelope, die Entscheidungsunterlagen und die Zeitstempel und lässt den befugten Betreiber zugleich die wirksamste Maßnahme mit den geringsten Kollateralauswirkungen wählen.

01 · INGEST

Erfassen & bewahren

Meldungen und Beobachtungen erfassen; Rohartefakte hashen; Uhren synchronisieren.

02 · PROVENIENZ

Beweismittel standardisieren

Herkunft, Methode, Verarbeitungshistorie und Abhängigkeiten von Quellen dokumentieren.

03 · ÜBERPRÜFEN

Bestätigen

Das schädliche Verhalten nachstellen und unabhängige Beweise unterscheiden.

04 · BEURTEILEN

Risiko & Kollateralauswirkungen

Böswillige Registrierungen, kompromittierte Dienste, Shared Hosting und Schweregrad klassifizieren.

05 · ANTWORTEN

Benachrichtigen & Abhilfe schaffen

Den Verantwortlichen, den Zieltermin und die wirksamste Abhilfemaßnahme mit den geringsten Beeinträchtigungen festlegen.

06 · RÜCKBLICK

Prüfung und Einspruch

Metadaten zu den Ergebnissen veröffentlichen, die Wirkung messen und eine rasche Umkehrung unterstützen.

Evidenzstufen

E1 — **Nicht verifiziertes Signal**

Einzelner Hinweis, lexikalische Übereinstimmung oder Reputationsvorwurf. Geeignet zur Beobachtung, reicht allein jedoch niemals für eine Suspendierung aus.

E2 — **Reproduziertes Verhalten**

Mit Zeitstempel versehene Aufzeichnung von Credential-Diebstahl, Malware-Auslieferung oder einem irreführenden Transaktionspfad.

E3

Unabhängige Bestätigung

Mindestens zwei wirklich unabhängige Quellen oder ein reproduzierbarer technischer Nachweis sowie Überprüfungen hinsichtlich Eigentumsverhältnissen und Kontext.

E4

Qualifizierte Bestätigung

Zuständige Behörde, betroffener Dienst, Markeninhaber oder validierte Opferbeweismittel mit datenschutzkonformer Beweismittelkette.

UNABHÄNGIGKEITSREGEL

Drei Feeds, die dieselbe vorgelagerte Blacklist kopieren, stellen eine Quelle dar, nicht drei. Der Provenienzgraph muss die gemeinsame Herkunft, die Synchronisation und die erneute Veröffentlichung durch den Anbieter aufzeigen.

11 Ein minimaler Evidence Envelope und eine interoperable API

Die „API“ sollte einen überprüfbaren Fall anlegen und einen nachprüfbaren Reaktions-Timer starten; ein Melder darf keinen Haltebefehl direkt erteilen können. Betrifft ein E3/E4-Fall eine böswillige Registrierung mit einem einzigen Zweck und läuft er ohne begründete Entscheidung oder wirksame Abhilfemaßnahmen ab, eskaliert das System ihn automatisch an den Registrierungsbetreiber oder einen anderen Akteur mit vertraglicher oder gesetzlicher Befugnis. A `serverHold` Ein Befehl darf nur von einem autorisierten Akteur stammen. Die automatische Eskalation und die Befugnis der Registrierungsstelle, bei Ablauf Maßnahmen zu ergreifen, sind vorgeschlagene Richtlinienänderungen und stellen keine Behauptungen über bestehende Befugnisse dar. Jeder Zustandswechsel wird signiert und dem Prüfprotokoll angehängt.

POST /V1/CASES · BEISPIEL

```
{
  "indicator": {"type": "domain", "value": "example.invalid"},
  "alleged_category": "credential_phishing",
  "observed_at": "2026-08-02T06:14:22Z",
  "evidence": [
    {
      "type": "http_capture",
      "sha256": "a3f1c9…",
      "collection_method": "isolated_browser_v2",
      "source_id": "reporter:ed25519:7c2a…"
    }
  ],
  "provenance_graph": "ipfs-or-object-store:sha256:91bd…",
  "collateral_context": {
    "registered_domain_scope": true,
    "shared_service": false,
    "mail_observed": true,
    "suspected_compromise": false
  },
  "requested_action": "review",
  "reporter_signature": "ed25519:…"
}
```

Eine erfolgreiche Antwort enthält eine Fall-ID, den empfangenden Akteur, die Nachweisstufe, Fehler hinsichtlich der Vollständigkeit, die voraussichtliche Bearbeitungszeit sowie eine öffentliche Transparenz-URL. Es darf keine konkrete Abhilfemaßnahme zugesagt werden, bevor ein zuständiger Akteur die Zuständigkeit und die Nebenwirkungen geprüft hat.

12 Vorgeschlagene Reaktionsziele, keine allgemeingültigen Abschaltfristen

Service-Level-Ziele sollten *Eingangsbestätigung*, *Triage*, *Entscheidung* und *wirksame Risikominderung* getrennt messen. So wird Leistung vergleichbar, ohne eine Sperrung stets als richtige Folge zu unterstellen.

FALLPROFIL	BESTÄTIGEN	TRIAGE-ZIEL	ENTSCHEIDUNGSZIEL	TYPISCHE ANTWORTMÖGLICHKEITEN
E3/E4-Diebstahl von Zahlungsdaten oder Seed-Phrasen durch eine böswillige Registrierung mit nur einem Zweck	15 Min.	1 Stunde	4 Std.	Inhalt sperren; Registrar- oder Registry-Hold, sofern befugt; Browser- und Zahlungswarnungen.
E3-Markenphishing oder Malware-Auslieferung	30 Min.	2 Std.	6 Std.	Host-/CDN-Abschaltung, Domain-Risikominderung, Sinkhole oder Warnung je nach Kontrollpunkt.
Kompromittierte legitime Domain oder gemeinsamer SaaS-Mandant	1 Stunde	4 Std.	12 Std.	Pfad-/Kontoisolierung und Wiederherstellung der Eigentumsrechte; die Sperrung registrierter Domains sollte nach Möglichkeit vermieden werden.
Finanzbetrug mit umstrittener Einstufung	4 Std.	12 Std.	24 Std.	Sicherung, Maßnahmen auf Plattform- und Zahlungsebene, Weiterleitung an die zuständige Behörde und begründete Entscheidung.
E1-Signal oder unvollständiger Bericht	Auto	24 Std.	Keine, bis zur Validierung	Überwachen, ergänzen und Nachweise anfordern.

Dies sind vorläufige Zielwerte. Die korrekten Werte sollten anhand der beobachteten Bedrohungsdauer, des Personalbedarfs, der Fehlerkosten und der rechtlichen Vorgaben ermittelt und anschließend nicht als einfacher Durchschnittswert, sondern als Erreichungsverteilung veröffentlicht werden.

13 Sicherheit, ordnungsgemäßes Verfahren, Datenschutz und Fehlerfälle

Eine schnelle Reaktion ohne Sicherheitsvorkehrungen kann fehlerhafte Daten zu Zensur, wirtschaftlicher Sabotage oder Infrastrukturausfällen eskalieren lassen. Eine solide Architektur behandelt daher Fehlalarme und Kollateralschäden als schwerwiegende Sicherheitsversagen.

FEHLERMODUS	ERFORDERLICHE STEUERUNG	ÜBERPRÜFBARE MASSNAHME
Böswillige Meldung gegen einen Wettbewerber	Authentifizierung der Meldenden, Quellenreputation, unabhängige Reproduktion und Sanktionen bei Missbrauch	Anteil abgelehnter Meldungen je meldender Stelle; bestätigte Manipulationsfälle
Als Konsens erscheinende Zirkularität von Feeds	Provenienzgraph und Deduplizierung vorgelagerter Quellen	Zahl unabhängiger Quellen vor und nach Korrektur der Datenherkunft
Kompromittierte legitime Domain pauschal gesperrt	Klassifizierung der Registrierungsabsicht und Präferenz für Abhilfemaßnahmen auf Pfadebene	Anteil der kompromittierten Domains; betroffene legitime Dienste
Daten zu Opfern oder Details zu Sicherheitslücken wurden öffentlich bekannt	Gestaffelte Offenlegung, Schwärzung, versiegelte Beweismittel und Aufbewahrungsfristen	Vorfälle im Zusammenhang mit dem Datenschutz; Ergebnisse der Überprüfung der Schwärzungen
Eine unrechtmäßige Maßnahme bleibt bestehen	Rund-um-die-Uhr-Eingang für Einsprüche, unabhängige Prüfung und authentifizierter Wiederherstellungsprozess	Median und 95. Perzentil der Aufhebungszeit
Ein Registry-Hold unterbricht E-Mail oder Subdomains	Bestandsaufnahme möglicher Kollateralauswirkungen, Verhältnismäßigkeit der Abhilfe und Überwachung nach der Maßnahme	Beeinträchtigte Dienste je Maßnahme; Aufhebungsrate

Mindestgarantien für ein ordnungsgemäßes Verfahren

1. Für jede einschränkende Maßnahme werden der Grundcode, die Nachweisstufe und der zuständige Entscheidungsträger erfasst.
2. Ein Registrant kann eine datenschutzkonforme Begründung einholen und Gegenbeweise vorlegen.
3. Eilbeschwerden werden von einer Person geprüft, die die ursprüngliche Entscheidung nicht getroffen hat.
4. Die Aufhebung wird über denselben signierten Kanal weitergeleitet wie die ursprüngliche Maßnahme.
5. Gesamtstatistiken zu Fehlern und Wiederherstellungen sind öffentlich zugänglich; sensible Beweismittel unterliegen weiterhin einer Zugriffskontrolle.

14 Vom „Toxizitätswert“ zum aussagekräftigen Response-Quality-Index

Eine öffentliche Bewertung eines Registrars kann die Rechenschaftspflicht verbessern; naive Ranglisten werden jedoch durch Portfoliogröße, Quellenabdeckung, Kundenmix und die Unterscheidung zwischen böswilliger Registrierung und späterer Kompromittierung verzerrt. Eine Bewertung darf niemals die pauschale Sperrung aller Kunden eines Registrars rechtfertigen.

VORGESCHLAGENER QUALITÄTSVEKTOR

```
RQI = report as a vector, not a single opaque rank:

  coverage-adjusted validated-abuse rate
  median / p90 acknowledge, triage and decision times
  mitigation effectiveness and recurrence
  false-positive and reversal rates
  median / p95 appeal-resolution time
  evidence completeness and transparency rate

Always publish N, observation window, confidence intervals,
feed coverage and malicious-registration / compromise split.
```

Wenn für die Governance ein zusammengesetzter Index erforderlich ist, sollten vor der Auswertung Gewichtungskoeffizienten festgelegt, Sensitivitätstests durchgeführt und Backtests anhand von aus der Auswertung ausgeschlossenen Fällen vorgenommen werden. Die Ergebnisse sollten nach TLD, Größe der Registrierungsstelle, Bedrohungsklasse und Quelle der Nachweise aufgeschlüsselt werden. Das Ergebnis ist ein Signal zur Rechenschaftspflicht – kein automatisiertes Urteil über eine Domain.

15 Eine mehrstufige öffentliche Transparenzdatenbank für DNS Abuse

Ein Transparenzregister kann Streitigkeiten darüber ausräumen, ob eine Benachrichtigung vorlag, wann sie zugestellt wurde und welche Maßnahmen daraufhin ergriffen wurden. Die Veröffentlichung aller Belege könnte jedoch Opfer, personenbezogene Daten, Ermittlungsmethoden und aktuelle Angriffswege offenlegen. Die Lösung ist ein gestaffelter Zugriff.

P

Öffentliches Register

Fall-ID, Indikator, Oberkategorie, zentrale Zeitstempel, Beweisstufe, Rollen der Akteure, Ergebniscode, Einspruchsstatus und Hashes versiegelter Artefakte.

C

Sichtweise des Vertragspartners

Reproduzierbare technische Nachweise, Kontaktkanal, Begleitkontext und Anweisungen zur Aufbewahrung.

R

Eingeschränkte Behördenansicht

Opferdaten, finanzielle Zuordnung, Material aus laufenden Ermittlungen und die ungeschwärzte Beweismittelkette.

Jedes Update ist nur anfügbar, mit einem Zeitstempel versehen und signiert. Korrekturen löschen den Verlauf nicht, sondern fügen einen neuen Eintrag hinzu, der den alten ersetzt. Die öffentliche Suche sollte die Aufbewahrungsvorschriften einhalten, eine massenhafte Identifizierung von Betroffenen verhindern und Abhilfe bei unrichtigen personenbezogenen Daten bieten.

16 Ein sechsmonatiger Pilotversuch mit vorab registrierter Evaluation

Ein aussagekräftiger Pilotversuch sollte klein genug für verlässliche Governance und groß genug zur Prüfung der Kausalkette sein. Vorgeschlagener Umfang: drei freiwillige Registrare, zwei Registry-Betreiber, ein Hosting-/CDN-Partner, zwei unabhängige Forschungsfeeds und ein qualifiziertes Einspruchsgremium. Studienprotokoll und Endpunktdefinitionen sollten vor der Fallzuweisung registriert werden.

MONAT 1

Protokoll und rechtliche Zuordnung

Kategorien, Zuständigkeiten, Nachweisschwellen, Datenschutz-Folgenabschätzungen und Beendigungsbedingungen definieren.

MONAT 2

Bestehenden Prozess instrumentieren

Ausgangszeitstempel und Ergebnisse messen, ohne das Reaktionsverhalten zu verändern.

MONAT 3

Evidence Envelope erproben

Signierte Provenienz, Deduplizierung und Klassifizierung von Kollateralauswirkungen einführen.

MONAT 4

Reaktionsziele testen

Geeignete Fälle randomisieren oder schrittweise einführen; Fehler täglich überwachen.

MONAT 5

Einsprüche und Fehlerfälle erproben

Wiederherstellungsübungen, böswillige Red-Team-Meldungen und Prüfungen der Zugriffskontrollen durchführen.

MONAT 6

Unabhängige Bewertung

Effektstärken, Konfidenzintervalle, Angaben zu fehlenden Werten, unerwünschte Ereignisse, Kosten und Materialien zur Reproduktion der Studie veröffentlichen.

Primäre Endpunkte der Pilotstudie

- Median und 90. Perzentil der Zeitspanne vom Vorliegen validierter Erkenntnisse bis zur wirksamen Eindämmung.
- Unterschied im zurechenbaren Schaden nach der Benachrichtigung oder einem vorab festgelegten Ersatzindikator für die Exposition der Betroffenen.
- Falsch-positiv-Rate, Schweregrad ungerechtfertigter Maßnahmen und mediane Wiederherstellungszeit.
- Wiederholung auf der Ebene desselben Registranten, Infrastruktur-Clusters und derselben Kampagne.
- Direkte Betriebskosten pro validiertem Fall und pro wirksamer Abhilfemaßnahme.

ENTSCHEIDUNGSREGEL

Eine Ausweitung sollte nur dann erfolgen, wenn der Pilotversuch eine deutlich schnellere effektive Schadensminderung nachweist, ohne dabei die vorab festgelegten Grenzwerte für Fehlalarme, Datenschutzvorfälle, Verzögerungen bei Einsprüchen oder damit verbundene Dienstunterbrechungen zu überschreiten.

17 Schlussfolgerungen und überprüfbare Empfehlungen

Die Reaktion auf DNS Abuse ist weder ein rein technischer Filter noch eine Aufgabe, die eine einzelne Institution allein lösen kann. Die geltenden Verträge von 2024 begründeten substanzielle Pflichten zur Risikominderung, lassen aber erheblichen Ermessensspielraum bei Beweismitteln, Zeitpunkt und Abhilfe. Dieser Spielraum ist für Verhältnismäßigkeit erforderlich; ohne vergleichbare Aufzeichnungen erschwert er zugleich die Leistungsbewertung.

1. **Evidence Envelope standardisieren.** Einheitliche Felder für Provenienz, Zeitstempel und Ergebnisse bei Meldenden, Registraren, Registries und Infrastrukturanbietern einführen.

2. **Die Etappen separat messen.** Veröffentlichen Sie die Zeiten für die Bestätigung, Triage, Entscheidung, Schadensminderung und Einspruch nach Bedrohungsklasse und Evidenzstufe.
3. **Unterscheiden Sie eine böswillige Registrierung von einer Kompromittierung.** Bei kompromittierten legitimen Diensten sollte vorrangig eine Behebung auf Pfad-/Kontoebene angestrebt werden; domänenweite Maßnahmen sollten nur in Fällen ergriffen werden, in denen sie verhältnismäßig sind.
4. **Reaktionsziele pilotieren.** Stundenbasierte Zielwerte für hochgradig gesicherte, ausschließlich böswillige Registrierungen testen, statt eine allgemeingültige Frist festzulegen.
5. **Veröffentlichen Sie datenschutzkonforme Daten zur Rechenschaftspflicht.** Verwenden Sie ein mehrstufiges Transparenzregister mit signierten Verlaufsdaten und eingeschränkten Nachweisen.
6. **Bewertung der kausalen Auswirkungen.** Man sollte eine schnellere Aussetzung nicht gleichbedeutend mit Kosteneinsparungen setzen, solange keine vorab registrierte Studie die Auswirkungen auf die Opfer und die Verlagerungseffekte untersucht hat.

Die konstruktive Schlussfolgerung lautet nicht, dass das ursprüngliche Problem verschwindet, sobald seine Behauptungen relativiert werden. Vielmehr können die zentralen Behauptungen nun überprüft werden: Der Schadensbereich von 60–85 % nach der Erkennung ist eine explizite quantitative Hypothese; 100–150 $ sind eine überprüfbare technische Budgetannahme für eine definierte Sensor- und Triage-Ebene; und Reaktionsziele im Stundenbereich können für hochgradig zuverlässige, zweckgebundene böswillige Registrierungen erprobt werden. Veröffentlichen Sie den Arbeitsaufwand, die Kosten, die Zeitstempel und die Ergebnisse, vergleichen Sie diese mit einer Basislinie und messen Sie Abweichungen und Fehler. Eine Bestätigung würde vertragliche und politische Änderungen rechtfertigen; eine Ablehnung würde aufzeigen, welche Annahme fehlgeschlagen ist.

Hinweise zur redaktionellen Bearbeitung und zu den Methoden. PhishDestroy ist ein unabhängiges, nichtkommerzielles Projekt zur Bedrohungsanalyse. Diese Veröffentlichung ist ein Vorschlag zu Richtlinien und technischen Lösungen und stellt weder eine Rechtsberatung noch ein „ICANN"-Programm oder eine begutachtete wissenschaftliche Arbeit dar. Als „Modelle" bezeichnete Budgetbereiche sind Planungsannahmen. Verweise auf Primärquellen sind unten verlinkt. Korrekturen können über die Kontakt- und Responsible-Disclosure-Kanäle der Website eingereicht werden.

DIE PERSPEKTIVE DER ERSTEN PERSON · VERANTWORTLICHKEIT MUSS SOWOHL UNTÄTIGKEIT ALS AUCH ÜBERGRIFFIGKEIT EINSCHRÄNKEN

Eine persönliche Grenze der Vollstreckungsbefugnis

Ich bitte nicht um – und möchte auch keinen – direkten Zugriff auf ein Tool zur Domain-Sperrung. Diese Befugnis erfordert eine unabhängige Überprüfung, öffentlich zugängliche Prüfprotokolle, ein zügiges Rechtsmittelverfahren und die Möglichkeit der Rückgängigmachung.

Ich bin der Meinung, dass es viele kompetente und verantwortungsbewusste Unternehmen gibt, denen man Teile dieser Arbeit anvertrauen könnte. Aufgrund meiner Erfahrungen und der von mir veröffentlichten Berichte zähle ich NameSilo nicht zu dieser Gruppe.

Ich würde seriösen US-Unternehmen davon abraten, sensible Aufgaben im Bereich Missbrauchsbekämpfung oder Sicherheit bestimmten Auftragnehmern anzuvertrauen, deren Interessenkonflikte, Kompetenz oder Verhalten einer unabhängigen Überprüfung nicht standhalten. Hier geht es um dokumentierte Handlungen, nicht um die Nationalität: Eine russische Herkunft allein beweist nichts, genauso wenig wie eine amerikanische Firmenadresse etwas beweist.

Ich will Gerechtigkeit und echte Rechenschaftspflicht für Registrare, die Einnahmen aus der Registrierung und Verlängerung von Domains erzielt haben, die im Rahmen wiederholter Betrugsaktionen dokumentiert wurden. Wenn die Beweislage über bloße Fahrlässigkeit hinaus auf eine mögliche wissentliche Beihilfe hindeutet – sei es durch direkte operative Beteiligung oder durch das Auftreten als informierter Vermittler, dessen Aufgabe darin bestand, eine schädliche Domain trotz wiederholter Warnungen registriert und online zu halten –, sollte dieses Verhalten unabhängig untersucht werden und, falls sich der Verdacht bestätigt, Konsequenzen nach sich ziehen. Ich stelle den Verdacht nicht als feststehende Tatsache dar; doch der Status als Vermittler darf keine Immunität vor einer Überprüfung gewähren.

Die zugrunde liegenden Ermittlungen prüfen ↗

A

Literaturverzeichnis und Quellenangaben

[1] **ICANN: Verabschiedeter Haushalt für das Geschäftsjahr 27 (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf

Quelle für die Betriebsmittel in Höhe von 165,1 Mio. $ für das Geschäftsjahr 27 und die Zusammensetzung der Finanzierungsquellen.

[2] **ICANN: Globale Änderung des Registrar Accreditation Agreement von 2024** · https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-global-amendment-05apr24-en.pdf

Primäre vertragliche Quelle für die Pflichten von Registraren im Zusammenhang mit DNS Abuse.

[3] **ICANN: Globale Änderung des Base Registry Agreement von 2024** · https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-global-amendment-05-04-2024-en.html

Primäre vertragliche Grundlage für die Mitigationspflichten des Registry-Betreibers.

[4] **ICANN Contractual Compliance: Leitfaden zu Pflichten bei DNS Abuse (2024)** · https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en
Operative Auslegung, Anforderungen an Meldungen und Beispiele angemessener Risikominderung.

[5] **ICANN: Umsetzung der Anforderungen zur Eindämmung von DNS Abuse (2024)** · https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf
Sechsmonatiger Umsetzungsbericht sowie Zahlen zu Untersuchungen und Risikominderung.

[6] **ICANN SSAC, SAC115: Bericht über einen interoperablen Ansatz zur Bearbeitung von Abuse-Meldungen (2021)** · https://www.icann.org/en/system/files/files/sac-115-en.pdf
Hintergrund zur Interoperabilität von Abuse-Meldungen und zur Qualität der Beweismittel.

[7] **Hollenbeck, RFC 5731: EPP-Domainnamen-Zuordnung (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html
Technische Definition der Statuswerte der EPP-Domäne, einschließlich der vom Server festgelegten Statuswerte.

[8] **Laurie et al., RFC 9162: Certificate Transparency Version 2.0 (2021)** · https://www.rfc-editor.org/rfc/rfc9162.html
Maßgebliche Protokollspezifikation und Grenzen der CT als Sensor.

[9] **ICANN, Zentraler Zonendatendienst** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service
Gültigkeitsbereich und Zugriffsmodell für die an „gTLD“ beteiligten Zonendateien.

[10] **FBI Internet Crime Complaint Center, IC3-Jahresbericht 2025** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
Zahlen zu Beschwerden und gemeldeten Schäden, einschließlich der Fälle von Phishing und Spoofing.

[11] **Bijmans et al., „Catching Phishers By Their Bait“ (USENIX Security, 2021)** · https://www.usenix.org/system/files/sec21-bijmans.pdf
Datensatzspezifische Messungen der Phishing-Infrastruktur und der beobachteten Lebensdauer.

[12] **Neu registrierte Domains und die Lebensdauer von Phishing-Seiten, Journal of Cybersecurity (2026)** · https://doi.org/10.1093/cybsec/tyag020
Aktuelle empirische Erkenntnisse zu neu registrierten Phishing-Domains und deren Verteilung über die gesamte Lebensdauer.

[13] **Inferenzanalyse böswillig registrierter Domains – INFERMAL (2024)** · https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

ICANN-finanzierte Analyse böswilliger Registrierungen und von Ökosystemfaktoren; relevante Grenzen für Kausalaussagen.

[14] **Chainalysis: Trends bei Krypto-Betrugsfällen im Jahr 2026** · https://www.chainalysis.com/blog/crypto-scams-2026/

Schätzung eines Anbieters zu den Betrugszuflüssen über die Blockchain im Jahr 2025; wird nicht als Gesamtwert für Domain-Phishing gewertet.

[15] **APWG, Bericht zu Trends bei Phishing-Aktivitäten, 1. Quartal 2026** · https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf

Festgestellte Phishing-Angriffe/URLs; die Kennzahlen entsprechen nicht der Anzahl der registrierten Domains.

[16] **Informationszentrum für Cyberkriminalität / Interisle, Phishing-Landschaft 2025** · https://www.cybercrimeinfocenter.org/phishing-activity-numbers-may-april-2025

Unterscheidet zwischen beobachteten Angriffen, eindeutigen Domains und böswillig registrierten Domains.

[17] **Verisign, Branchenbericht zur Domainnamenbranche, 2. Quartal 2026** · https://blog.verisign.com/domain-names/q2-2026-domain-name-industry-brief-quarterly-report/

Quelle für die gemeldeten 401,6 Millionen Registrierungen über alle TLDs hinweg.