Switch

Rapport d’activité 2024

du registry pour les ccTLD .ch et .li

Table des matières

La couverture des coûts de l'infrastructure critique DNS ne peut plus être assurée exclusivement par l'augmentation des volumes.

Urs Eppenberger
Head of Registry, Switch

Switch

Éditorial

Urs Eppenberger, Head of Registry

Le monde des noms de domaine est en phase de consolidation. Les exploitants de registry, en particulier, espèrent un nouvel élan lors du prochain lancement de nouveaux noms de domaine de premier niveau (TLD) en 2026. Cela ne devrait toutefois guère avoir d'influence sur la quantité de noms de domaine .ch.

La période du coronavirus a accéléré la transition numérique. Cette phase est clairement terminée, les détenteurs privés consolident désormais leurs noms de domaine accumulés. Il en résulte une croissance totale plus faible et une baisse du chiffre d'affaires des registrars. Les actions publicitaires menées par les hébergeurs et les registrars pourraient sensibiliser les entreprises au fait qu'une présence Web individuelle avec leur propre nom de domaine renforce leur marque et leur permet de positionner leurs offres sous leur propre contrôle. En revanche, si les entreprises choisissent de proposer leurs produits ou services via les grandes plateformes de vente, elles n'ont pas besoin de leur propre site web ou d'un nom de domaine. Ces plateformes ont l'avantage d'être de grandes structures aux activités mondiales. Il est difficile d'estimer quel canal de vente sera gagnant.

Le débat sur la croissance ou la stagnation est important pour les registrars et le service d'enregistrement, car il s'agit de trouver les moyens de couvrir les coûts engendrés par le renchérissement, les exigences croissantes en matière de résilience de l'infrastructure et les prescriptions de conformité. La couverture des coûts ne peut plus être assurée exclusivement par l'augmentation des volumes.

Les 2,6 millions de noms de domaine enregistrés, les serveurs de noms et les résolveurs des fournisseurs d'accès Internet constituent une infrastructure importante pour l'économie suisse et la population. Il est essentiel de les entretenir et de les protéger. Les prescriptions à ce sujet figurent dans la cyberstratégie nationale et dans la loi sur les télécommunications. Les capacités techniques nécessaires sont disponibles au sein du service d'enregistrement et des registrars. En concertation avec les autorités concernées, nous identifierons et mettrons en œuvre les mesures les plus efficaces pour sécuriser et développer cette infrastructure.

1.
Rapport d’activité – fonctionnement

Switch

Lutte contre la cybercriminalité

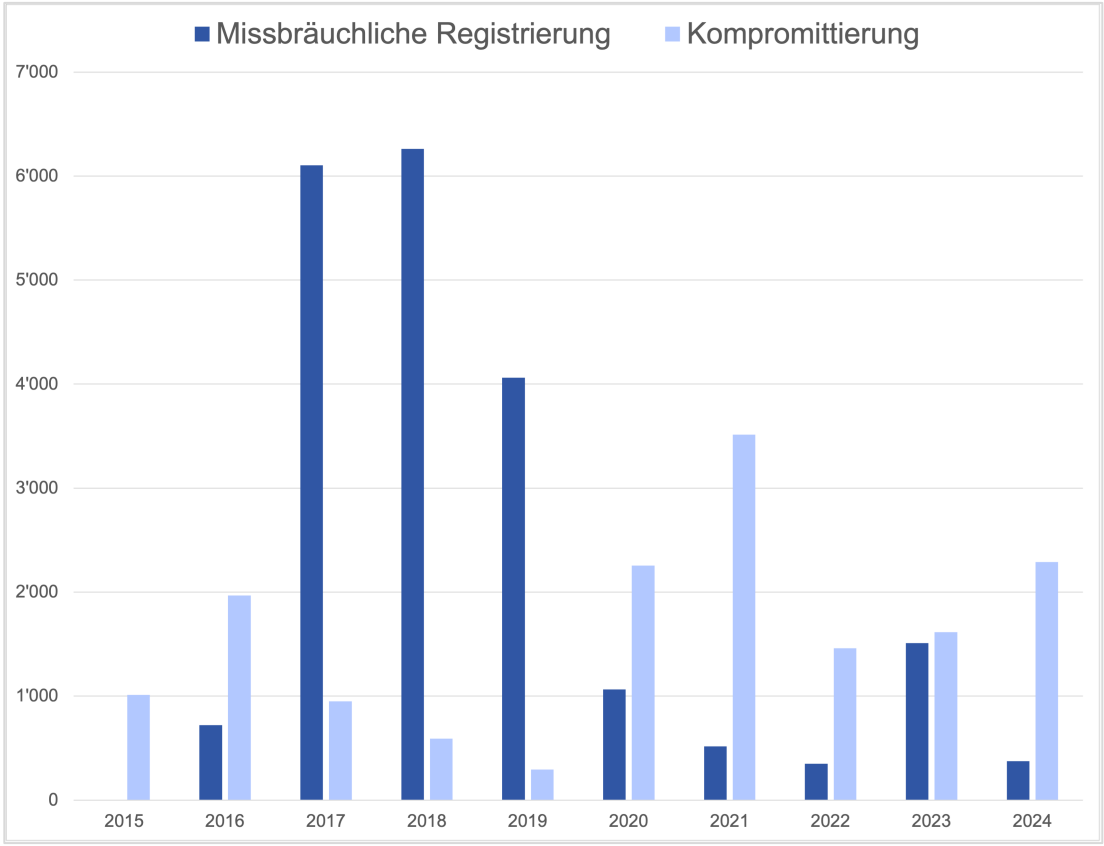
Pages Web compromises

Le nombre de pages Web compromises qui ont été utilisées à des fins de phishing et de malware a augmenté par rapport à l'année précédente. Une grande partie d'entre elles a été trouvée à l'aide du Web crawler spécialement développé pour la zone .ch.

Enregistrements abusifs

Le nombre de noms de domaine pour lesquels un soupçon d'enregistrement abusif a été signalé a diminué. Cela s'explique notamment par le fait que Fedpol a envoyé moins de demandes au titre de l'art. 15 ODI via son projet «SWITCHoff». Le nombre de demandes au titre de l'art. 16 ODI a également diminué.

Page Web: https://www.saferinternet.ch



Mesures en cas de suspicion d’abus

Demandes de la part d’autorités reconnues – art. 15.1 ODI

En 2024, les autorités accréditées ont envoyé au total 66 demandes de blocage immédiat (technique/administratif) de noms de domaine concernés par des cas de phishing en vertu de l’art. 15.1 de l’ODI. Il n’y a pas eu de cas de malware.

Demandes	Conséquence	2024
Sans réponse	Nom de domaine supprimé	65
Avec réponse	Nom de domaine réactivé	1
Total		**66**

Toutes les autorités reconnues par l’OFCOM sont répertoriées sur la page Web suivante: Autorités reconnues

Assistance administrative – art. 16.3 ODI

À la demande d’une administration intervenant dans le cadre de sa compétence, 310 demandes pour une adresse de correspondance en Suisse conformément l’art. 16.3 ODI ont été envoyées.

Demandes	Conséquence	2024
Sans réponse	Nom de domaine supprimé	246
Avec réponse	Nom de domaine réactivé	64
Total		**310**

Security Awareness – iBarry et SISA

En collaboration avec SISA, Switch sensibilise la population suisse. Avec trois nouvelles campagnes d'information (clés d'identification, nouvelle loi sur la protection des données, deepfakes), iBarry.ch contribue à diffuser des informations tout en offrant une orientation et un soutien en cas de doutes et de questions en lien avec la sécurité sur Internet.

https://checkawebsite.ibarry.ch

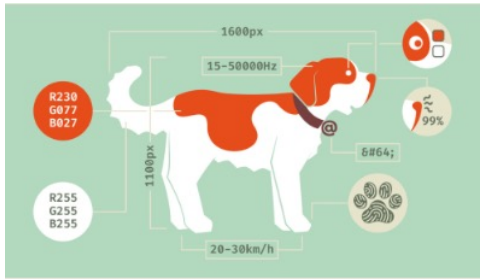
https://ibarry.ch

Afin d'optimiser l'offre pour la population suisse et de mieux positionner la plateforme iBarry, SISA a de nouveau participé à l'enquête auprès des internautes suisses de cette année.

https://cyberstudie.ch

Depuis cette année, la communauté iBarry reçoit une newsletter avec des informations actuelles.

→ S'inscrire ici



Security Awareness – anniversaire de SISA

Cette année encore, la Swiss Internet Security Alliance (SISA) s'est fixé pour objectif de mettre en réseau les principaux acteurs de la sécurité informatique en Suisse et de protéger la population.

Depuis le milieu de l'année, les membres de SISA peuvent obtenir des URL de cryptofraude supplémentaires via le flux de phishing existant. NEDIK collecte et partage ces données en collaboration avec Mute Group.

Nouveaux membres et partenaires en 2024:

NEDIK

CLUSIS 1989

Zürcher Hochschule für Angewandte Wissenschaften
zh aw

SBB CFF FFS

cyon

ISC2 CHAPTER

La SISA fête ses 10 ans

La Swiss Internet Security Alliance a été créée en 2014 par des représentants renommés de l'économie. Leur vision est de faire de la Suisse le pays Internet le plus sûr au monde.

Le conseil d'administration presque complet de la SISA (de g. à dr.): Simon Seebeck (Die Mobiliar), la présidente de la SISA Katja Dörlemann (Switch), Rita Frei (Sunrise), Marcus Beyer (Swisscom). Absent de la photo: Fabian Ilg (Prévention Suisse de la Criminalité). Photo: Netzmedien

Security Awareness Day

Le 24 octobre 2024, Switch a organisé pour la septième fois le Swiss Security Awareness Day. Cette année, la conférence, qui ne cesse de se développer, a de nouveau été organisée en partenariat avec iBarry.ch. Entre les conférences passionnantes, les quelque 130 participantes et participants ont pu rencontrer d'autres experts et échanger avec eux lors de diverses pauses networking.

Pour la première fois, des ateliers pratiques étaient également proposés.

Cette année encore, le programme visait à renforcer la compréhension du thème de la Security Awareness au sein de la communauté Switch et au-delà, tout en véhiculant de nouvelles idées et en favorisant les échanges.

Toutes les conférences sont en ligne.

Security Awareness Adventures

Les Switch Security Awareness Adventures

«Hack The Hacker – l'Escape Room» était la première des trois Security Awareness Adventures de Switch, suivie de «Track The Hacker – la chasse au trésor» et de «Piece of Cake – le jeu de rôle». Ces aventures jouissent toujours d'une grande popularité.

En 2024, Switch a organisé 77 de ces formations ludiques à la sécurité, soit presque le double par rapport à 2023 (40 sessions), et a partagé son expertise en matière de jeux d'entraînement lors de nombreuses conférences.

Site web: https://www.switch.ch/fr/security-awareness

Security Awareness – podcast

Podcast: Security Awareness Insider

En décembre 2024, le 50e épisode du podcast «Security Awareness Insider» (en allemand) a été publié.

Dans ce podcast, Katja Dörlemann (Switch) et Marcus Beyer (Swisscom) parlent de la sensibilisation des collaboratrices et des collaborateurs aux questions de sécurité ainsi que des moyens, outils et approches de formation nouveaux et créatifs. Ils donnent aussi un aperçu des programmes de Security Awareness des entreprises et des organisations, et bien plus encore.

Depuis son lancement, le podcast a déjà été téléchargé 25 000 fois, et chaque épisode enregistre désormais en moyenne 450 téléchargements.

Disponible partout où il y a des podcasts ou ici:
https://www.securityawarenessinsider.ch

Swiss Web Security Day

Le 29 octobre 2024, Switch a organisé le Swiss Web Security Day à Berne en collaboration avec SISA et Swico, en parallèle à l'événement LEO avec les autorités de poursuite pénale suisses. Avec 79 participantes et participants venus de Suisse et d'ailleurs, l'événement a remporté un franc succès et a reçu un écho très positif.

Le matin, l'unité centrale Cybercrime Bayern a donné une conférence sur la fraude aux investissements cryptographiques. Une deuxième conférence portait sur le thème «Internet-wide deployment of Post Quantum Cryptography for security protocols».

L'après-midi, des conférences ont notamment eu lieu sur le thème de l'abus de DNS ainsi que la présentation d'un litige au cours duquel l'autorégulation du secteur suisse de l'hébergement (Code de conduite Noms de domaine CCD de Swico) a été confirmée.

Comme l'année dernière, l'événement s'est déroulé exclusivement sur place, à Berne.

Katja Dörlemann, présidente de la SISA, Urs Eppenberger, Head of Registry Switch, Claudius Röllin, représentant de Swico IG Hosting.
Photo: Netzmedien

Événement LEO – Collaboration avec les autorités de poursuite pénale

Groupe-cible

Afin de continuer à soutenir les autorités dans leur lutte contre la cybercriminalité, Switch a lancé pour la quatrième fois l'événement LEO. LEO signifie «Law Enforcement Organizations».

Le 29 octobre 2024, la Law Enforcement Community s'est réunie à Berne afin de renforcer la communauté et d'encourager la création de partenariats avec des CERT du secteur privé. Cette coopération est essentielle dans la lutte contre la cybercriminalité.

C'est pourquoi non seulement la communauté LEO (59 personnes) a été invitée, mais aussi des représentants des CERT suisses (CH-CERT, 40 personnes). De nombreux participants étaient déjà présents l'année dernière et sont venus accompagnés de leurs collègues intéressés.

La répartition entre les régions était très équilibrée. Les participantes et participants provenaient des polices, des ministères publics ainsi que de la police nationale du Liechtenstein. Des autorités telles que Swissmedic, le Seco, la Finma et l'OFCOM étaient également représentées.

Thèmes

Différents thèmes ont été abordés. Les participantes et participants ont parlé des développements et des projets actuels concernant l'utilisation abusive des noms de domaine et la cybercriminalité. Les processus et les interfaces visant à simplifier la collaboration ont également été discutés.

L'accent a été mis sur la collaboration avec les parties prenantes concernées au-delà de la communauté afin de prévenir la cybercriminalité. Différents cas ont ainsi pu être résolus avec succès et efficacité grâce à cette coopération.

Résonance

L'événement a rencontré un franc succès. Les échanges dans le cadre de la collaboration ont nettement augmenté. On constate chaque année un grand intérêt. Les participantes et participants souhaitent une autre manifestation en 2025. Nous nous concentrerons davantage sur des exemples concrets afin de promouvoir cette coopération interdisciplinaire.

Fonctionnement du registry

Interruption du système d’enregistrement

Le système d’enregistrement a été interrompu le 19 janvier 2024. Entre 07h50 et 08h39, l’interface EPP n’était pas disponible pour les registrars. Une commutation sur le système de veille a permis de remédier à cette interruption.

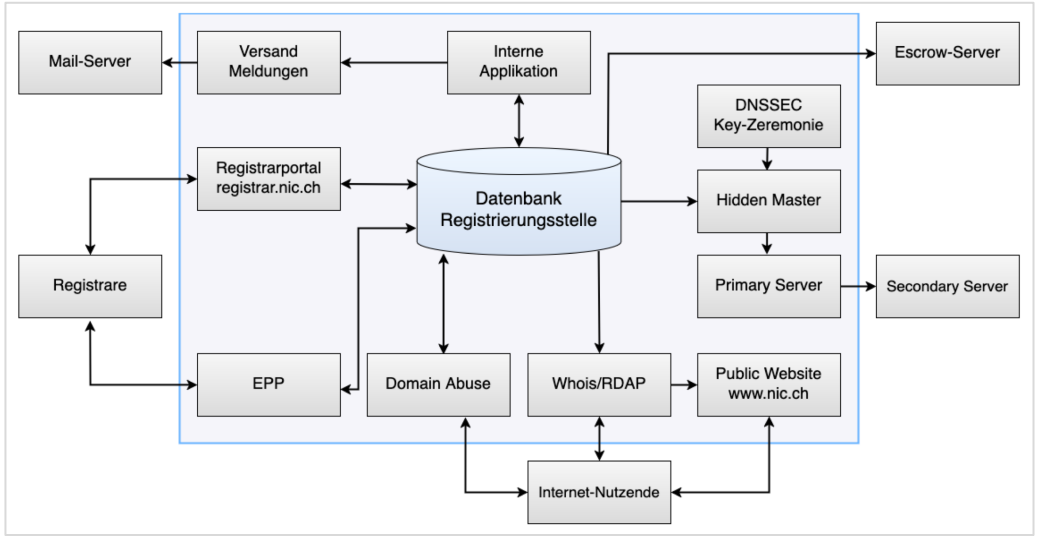
Le dysfonctionnement a été causé par une erreur de manipulation lors d’une maintenance standard planifiée sur la plateforme serveur subordonnée à Lausanne. La base de données centrale ayant été touchée par cette erreur, une commutation automatique sur le système de veille à Zurich n’a pas été possible.

Après un temps d’arrêt de 49 minutes, l’application d’enregistrement à Zurich a été réactivée sans perte de données. Les serveurs de noms n’ont pas été affectés par la panne et le fichier de zone était toujours à jour.

Défaillance du Registration Data Directory Service (RDDS)

Une erreur logicielle sur le serveur Whois a entraîné des entrées de journal excessivement volumineuses en raison de connexions/clients défectueux, ce qui a fini par remplir le disque dur. Cela a conduit à l’arrêt du serveur sur lequel sont mis à disposition les services whois.nic.ch et rdap.nic.ch. La gestion et l’attribution des noms de domaine n’ont pas été affectées par ce dysfonctionnement.

Vue d’ensemble du système du service d’enregistrement



European TLD ISAC

Le European TLD Information Sharing and Analysis Centre (ISAC) a été créé sous l'égide de CENTR en 2023.

Le Centre européen d'échange et d'analyse d'informations sur les domaines de premier niveau (European Top Level Domain Information Sharing and Analysis Center, TLD ISAC) vise à renforcer la sécurité et la résilience des services d'enregistrement de domaines de premier niveau en Europe par l'échange d'informations, la coopération et le partage des meilleures pratiques.

Il réunit les exploitants, les professionnels de la sécurité et d'autres parties prenantes afin d'échanger des informations sur les menaces, d'identifier les nouvelles tendances et de développer des mesures proactives pour prévenir et contrer les cyberattaques.

Switch est, avec d'autres exploitants de ccTLD européens, membre fondateur et membre actif du comité de pilotage, du groupe de travail et du groupe de Threat Intelligence Sharing.

Page web: https://www.tld-isac.eu

Tous les membres de CENTR ont été invités à donner leur évaluation des risques, de la gestion des risques et des conséquences possibles. Switch y a également participé. Les résultats ont été consolidés et résumés dans un rapport (Threat Landscape Analysis). Switch a comparé les 10 principaux risques qui en résulte avec sa propre carte des risques. Deux risques manquants et plausibles ont été inclus dans la gestion des risques propre à Switch.

EUROPEAN TLD ISAC

Abus à l’échelle mondiale

Suspension des rapports DAAR de l’ICANN

Switch a participé volontairement au projet DAAR de l’ICANN et a ainsi obtenu un rapport personnalisé sur l’utilisation abusive des noms de domaine pour .ch et .li. L’ICANN a suspendu les rapports au T1 2024.

L’ICANN a lancé un projet de suivi appelé Domain Metrica, dans un premier temps pour les gTLD. La participation des ccTLD n’est pas encore possible, mais nous suivons de près l’évolution de la situation.

Rapports Netbeacon publics

Switch participe aux mesures du Netbeacon Institute.

En octobre 2024, la zone .ch occupe la 5e place parmi les ccTLD les plus sûrs avec un volume de plus d’un million de noms de domaine.

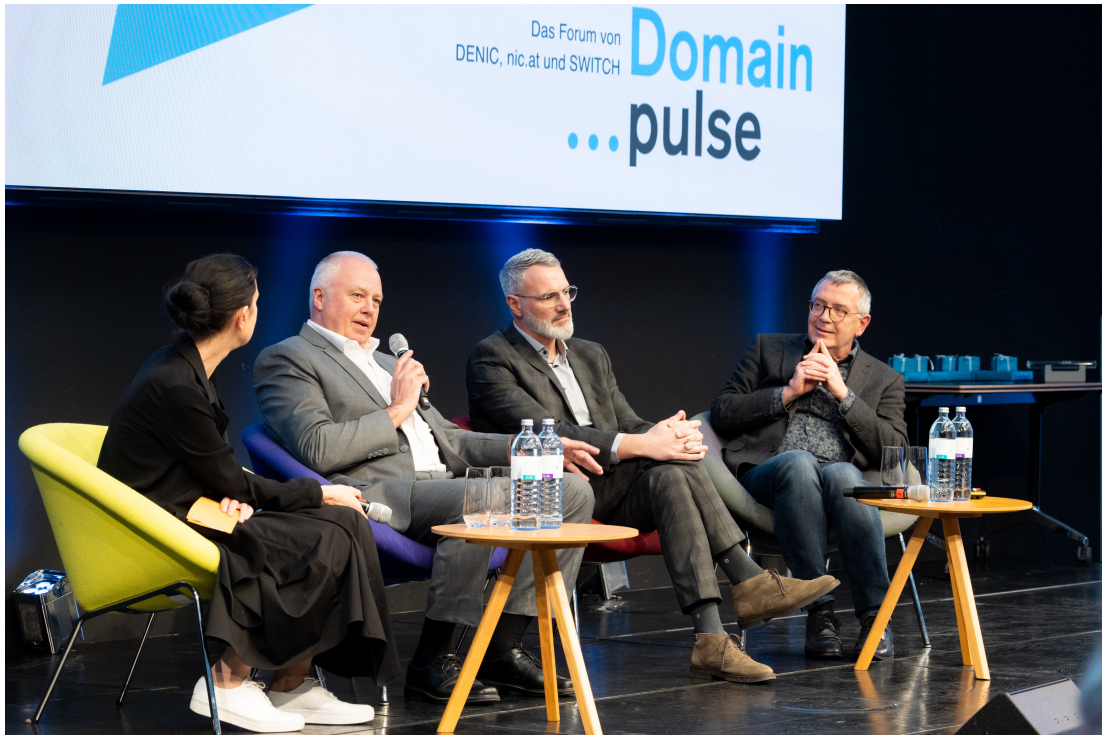
TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
nl	0.23	14	5,970,658
uk	0.28	28	9,870,870
it	0.37	12	3,222,803
at	0.41	6	1,457,415
ch	0.43	11	2,588,005
dk	0.46	6	1,317,284
ca	0.48	16	3,322,327
be	0.49	8	1,639,348
de	0.60	102	17,071,778
jp	0.64	11	1,713,367

Source: https://netbeacon.org/wp-content/uploads/2024/12/MAP-Report-December-2024-.pdf

Domain pulse 2024

Domain pulse s’est tenu à Vienne du 23 au 24 février 2024.

Sous la devise «Vienna Calling: Domain pulse 2024» ont été mis en lumière les possibilités, les limites et les effets des progrès techniques ainsi que des réglementations (NIS2) et des défis qui y sont liés. La sécurité et les mises à jour du secteur des domaines ont constitué un autre point fort.



Panel avec Richard Wein (directeur de nic.at), Andreas Musielak (membre du conseil d’administration de DENIC) et Urs Eppenberger (Head of Registry, Switch).

Programme de résilience DNS

50,4%

Au 1er janvier 2025, 50,4% de tous les noms de domaine .ch étaient signés.

Programme de résilience DNS

Résistance pour les noms de domaine .ch

Avec le programme de résilience DNS, Switch soutient l'introduction et la diffusion de normes de sécurité ouvertes pour les noms de domaine .ch et .li. Ces normes jouent un rôle clé dans l'augmentation de la résistance (résilience) face aux cybermenaces. Le programme, qui mise sur des incitations financières, se déroulera de 2022 à 2026.

L'objectif principal est d'encourager la signature des noms de domaine avec DNSSEC. Un supplément sera perçu pendant la durée du programme pour les noms de domaine qui ne sont pas signés ou qui le sont de manière erronée.

C'est le «DNSSEC Advisory Board» qui décide des normes de sécurité à promouvoir. Cet organe est composé de représentants de l'OFCOM, des registrars et de Switch.

Pour l'année 2024, le programme a été augmenté par les normes de sécurité des e-mails DMARC et SPF. En d'autres termes, en 2024, le remboursement des recettes supplémentaires se base non seulement sur DNSSEC, mais également sur l'implémentation réussie de DMARC et SPF.

L'Advisory Board a déjà décidé qu'en 2025, DANE et en 2026, IPv6 seraient encouragés en plus de DNSSEC.

Mesures de contrôle de la qualité

La vérification de l'implémentation correcte des normes de sécurité s'effectue en collaboration avec le prestataire de services externe OpenIntel. Pour tous les noms de domaine .ch et .li avec serveurs de noms, il est vérifié quotidiennement si les critères définis par le programme sont remplis. Les résultats de ces vérifications sont transmis à Switch. Les registrars avec des configurations erronées reçoivent des rapports d'erreurs afin de résoudre les problèmes.

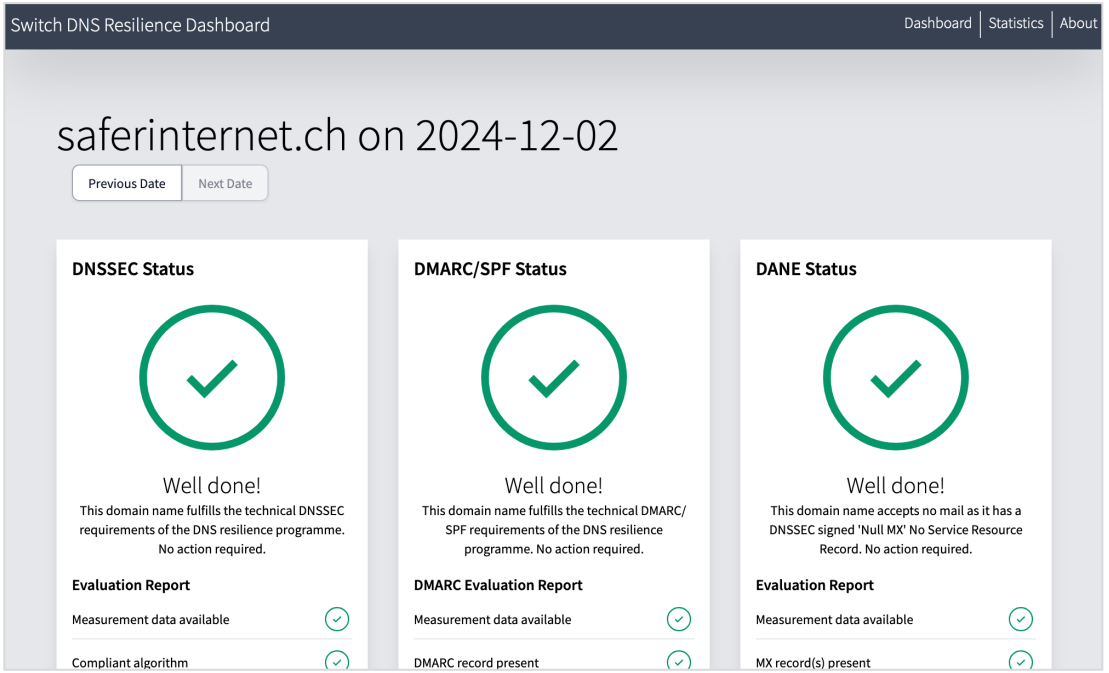
Programme de résilience DNS

Également au cours de sa troisième année d'exploitation, nous n'avons cessé de nous occuper du développement du programme de résilience, en plus de l'exploitation.

Évolutions 2024

- Augmentation de l'implémentation de DMARC/SPF.
- Mesures continues pour DMARC/SPF, envoi des rapports d'erreurs correspondants.
- Remboursements pour 2023 aux registrars autorisés sous forme de notes de crédit (fin février 2024).
- Implémentation des mesures pour DANE, ce critère sera pertinent en 2025.
- Envoi des nouveaux rapports d'erreurs pour DANE aux registrars depuis septembre 2024. Cela leur a permis de se préparer à 2025.
- Extension du Dashboard pour DANE chez le prestataire de mesure OpenIntel (voir capture d'écran ci-dessous avec le résultat pour le nom de domaine saferinternet.ch).
- Information continue des registrars, réponse à leurs demandes, assistance.

Les chiffres du programme de résilience se trouvent à la page 40.



Sites DNS Anycast et génération de la zone

Sites Anycast

Avec nos partenaires d'hébergement Anycast, la zone DNS est répartie sur plus de cent sites dans le monde. Celles-ci sont adaptées en permanence aux conditions actuelles. Depuis fin 2024, par exemple, il y a un nouveau nœud à Klagenfurt.

Génération de la zone

Depuis le passage de la configuration DNSSEC de NSEC3 à NSEC en 2023, aucune modification n'a été apportée au type de génération de la zone.

Audit ISO 27001 avec registries voisins

L’audit DACH a lieu trois fois par an, dans l’un des trois registries participants (DENIC, nic.at et Switch) et sous une conduite d’audit tournante. L’audit est suivi d’un échange sur les meilleures pratiques.

Le premier rendez-vous a eu lieu fin avril à Francfort chez DENIC (denic.de). DENIC et sa filiale, Denic Services, ont été audités pendant trois jours. La direction était assurée par nic.at.

Début juillet, le groupe d’audit s’est réuni chez Switch. Switch a été auditée sous la direction du CISO de DENIC, avec le soutien des ISO d’Allemagne et du service d’enregistrement autrichien nic.at.

Les résultats de l’audit sont pris en compte dans le processus d’amélioration continue et sont contrôlés par les auditeurs lors de l’un des audits suivants de la région DACH.

Sous la direction de Switch, un audit interne conforme à la norme ISO 27001:2022 a été réalisé du 24 au 26 septembre 2024 auprès du service d’enregistrement autrichien nic.at. Des représentants de DENIC étaient également présents.

Bien qu’il s’agisse d’un audit interne amical, les mêmes approches rigoureuses ont été appliquées que lors d’un audit externe régulier. nic.at a confirmé le haut niveau de maturité de ces dernières années et a démontré, grâce à des améliorations continues, qu’il est capable de répondre à ses exigences élevées en matière de conformité aux normes.

Après l’audit, les discussions se sont approfondies autour des exigences des normes et des possibilités de les mettre en œuvre de la manière la plus efficace et la plus conforme possible à l’aide de mesures techniques et organisationnelles.

DACH signifie Allemagne (D), Autriche (A), Suisse (CH).

ISMS – audit de surveillance ISO 27001

L'audit de surveillance ISO 27001 a eu lieu le 5 septembre dans les locaux du CSCS (Swiss National Supercomputing Centre) à Lugano.

Différents contrôles issus de la nouvelle norme ISO 27001:2022 ont déjà été vérifiés, notamment Threat Intelligence. Grâce à sa longue expérience de l'exploitation de CERT, Switch a pleinement convaincu l'auditeur. Security Architecture Governance et Procurement figuraient notamment parmi les autres thèmes abordés.

Le certificat a été délivré selon la norme de 2013.

Conclusion de l'auditeur: «La sécurité de l'information est un atout important pour Switch. Les connaissances techniques élevées et la sensibilisation à la sécurité de l'information de tous les collaborateurs interviewés sont frappantes.»

SV Cert.

IAF

SNAS
Reg. No. 661/R-141

ZERTIFIKAT

Nr. 860-ISMS-23

Rev.1

Hiermit wird bestätigt, dass das Managementsystem der

SWITCH

Werdstrasse 2 - 8021 - Zürich (Zürich, Switzerland)

Geschäftsstellen:
Werdstrasse 2 - 8021 - Zürich (Zürich, Switzerland)

die Anforderungen der Norm für das Information Security Management Systems

ISO/IEC 27001:2013

für folgenden anwendungsbereich erfüllt:

Domain Namen Registrierung

SOA Ausführung	Erstausgabedatum	Datum der Änderung	Ablaufdatum des Zertifikats
Version 1.7 vom 17.07.2024	05/12/2017	13/09/2024	05/12/2026

SV Cert. Group

Für die Zertifizierungsstelle
SV Certification Sro

(Gaetano Spera CEO SV CERT.)

Die Gültigkeit des Zertifikats unterliegt einer regelmäßigen jährlichen Überwachung und einer vollständigen Überprüfung des Systems alle drei Jahre.
Die Verwendung und Gültigkeit dieses Zertifikats unterliegen der Einhaltung der Zertifizierungsbestimmungen der SV Certification Sro.

SV CERTIFICATION Sro, HQ: Karadžičova 8A Bratislava
Mestská Casť Ružinov 821 08 – SLOVAKIA
Info & Contact: svcertification.com – info@svgroupcert.ch

«La sécurité de l'information est un atout important pour Switch. Les connaissances techniques élevées et la sensibilisation à la sécurité de l'information de tous les collaborateurs interviewés sont frappantes.»

Rapport d'audit ISO 27001

2.
Rapport d’activité – nouveautés

Switch

Domain Abuse 4.0

Lutte moderne et prometteuse contre les abus

Comme mentionné dans le rapport annuel 2023, la solution logicielle actuelle de lutte contre la cybercriminalité n'est plus à la hauteur des défis croissants que pose la lutte contre l'utilisation abusive des noms de domaine.

C'est pourquoi, dans le cadre du projet «Domain Abuse 4.0», une nouvelle solution logicielle tournée vers l'avenir est développée, basée sur les technologies les plus modernes. L'équipe de projet développe une solution rapide, nécessitant peu d'entretien et hautement évolutive. Les processus sont également révisés, adaptés aux nouvelles réalités et nos experts sont formés à cet effet. Grâce à ces mesures, Switch conserve un rôle de premier plan mondial dans la lutte contre la cybercriminalité.

Une étape importante a été franchie

En 2024, le CERT et le registry ont mis en œuvre ensemble les composants centraux de la nouvelle solution logicielle. Les premiers workflows (processus contre les abus) y ont été mis en œuvre et testés.

À la fin de l'année, nous avons mis en service la première version de la nouvelle solution logicielle. Depuis janvier 2025, nous pouvons utiliser le nouveau logiciel pour envoyer des demandes d'identification selon les art. 29 et 30 ODI au détenteur d'un nom de domaine lorsque nous avons de bonnes raisons de soupçonner des informations erronées sur le détenteur.

Domain Abuse 4.0

Perspectives 2025

Grâce au succès de l'année 2024, nous sommes bien préparés pour mettre en œuvre les workflows restants d'ici fin 2025 et laisser notre ancienne solution logicielle prendre une retraite bien méritée.

Sur le côté droit figurent les principaux workflows et composants logiciels dont l'implémentation est prévue pour chaque trimestre 2025 et qui seront ensuite transférés progressivement dans l'exploitation.

Perspectives 2026

De nouveaux workflows et fonctionnalités seront mis en œuvre en continu. Une interface technique avec les autorités constituera une fonctionnalité envisagée. Cette interface permettra aux autorités de connecter notre solution logicielle à leurs systèmes et de nous envoyer des demandes de manière automatisée.

Workflows et composants qui seront implémentés en 2025

T1 2025

- Enregistrements à des fins purement abusives
- Feed Reader (réception de signalements d'abus)

T2 2025

- Pages Web compromises (phishing et malware)
- Connexion à saferinternet.ch

T3 2025

- Demandes de blocage des autorités selon l'art. 15 ODI
- Reporting automatisé

T4 2025

- Demandes d'adresses de correspondance des autorités selon l'art. 16 ODI

T1 2026 Développement en cours

Reliability Engineering

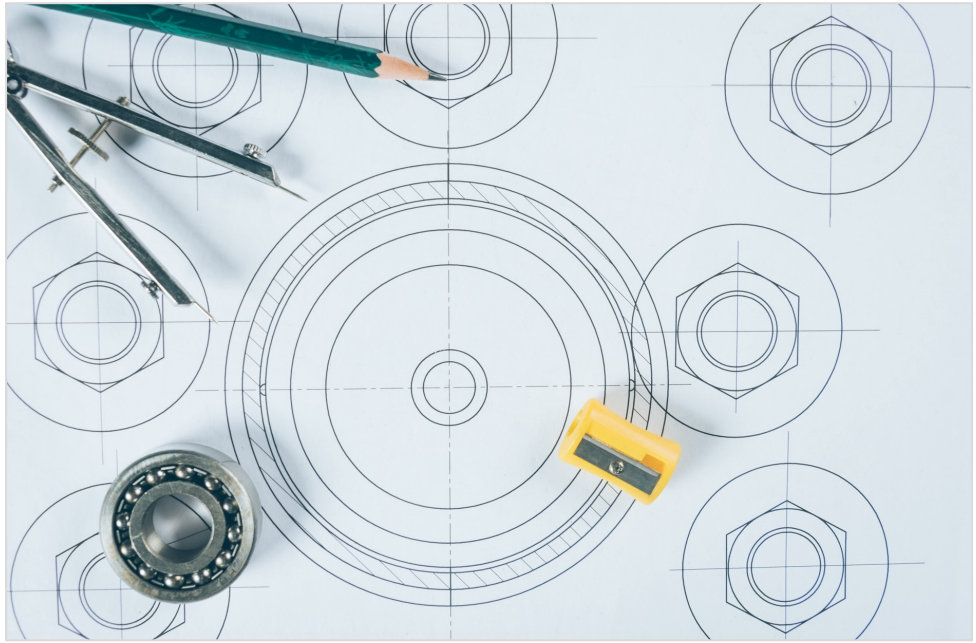
Les systèmes informatiques devenant de plus en plus complexes et s'intégrant de plus en plus dans nos vies, l'exploitation évolue elle aussi.

Pour compléter la sécurité de l'information, Switch introduit le concept de «Reliability Engineering», ainsi qu'un rôle spécial de coach ITSM et Reliability, afin que les équipes puissent fournir des services stables et fiables.

Nous nous concentrons sur des méthodes automatisées et évolutives pour gérer la disponibilité, la capacité ainsi que la gestion des incidents et des changements.

De nouveaux processus et directives ont été développés pour la gestion des incidents, celle des changements et la surveillance, et 15 formations spécialisées ont été organisées, notamment pour les membres de l'équipe Infrastructure et de l'équipe Senior Management.

«L'espoir n'est pas une stratégie. La chance n'est pas un facteur. La peur n'est pas une option.» James Cameron



Intégration ISMS – DSMS

Les normes ISMS (ISO 27001) et DSMS (ISO 27701) se recoupent largement.

D'une part, elles utilisent le même système de gestion de l'ISO, d'autre part, la norme DSMS n'est qu'un complément à la norme ISMS. C'est pourquoi les deux conseils d'administration compétents ont décidé de fusionner les deux concepts.

La nouvelle structure s'appelle désormais «Système de gestion intégré» ou IMS en abrégé. Pour le moment, Switch ne souhaite pas obtenir la certification ISO 27701.

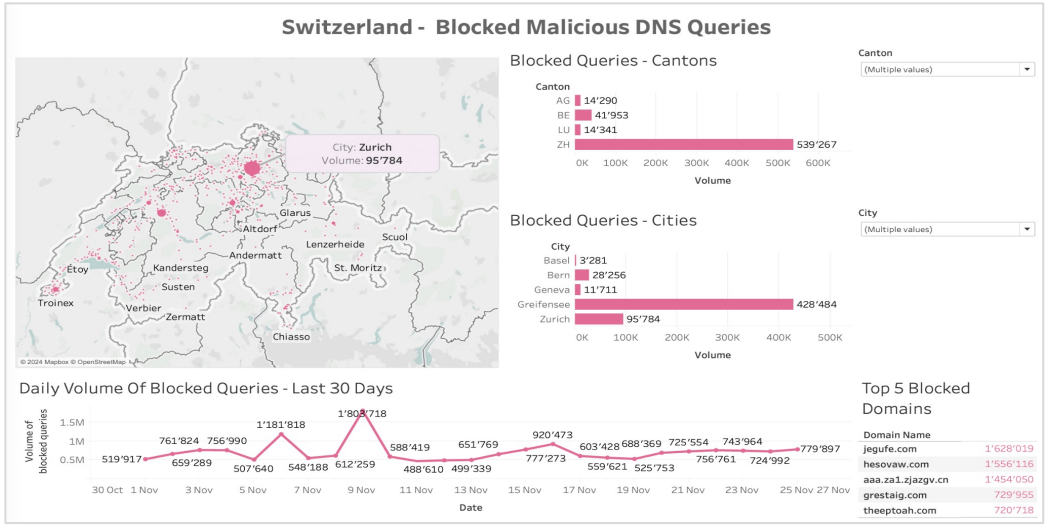
La fusion permet toutefois d'éviter les doublons dans la documentation. Cela simplifie également la formation des collaborateurs, car toutes les informations nécessaires se trouvent désormais au même endroit.

ISMS: Information Security Management System (Système de gestion de la sécurité de l'information)
DSMS: Data Protection Management System (Système de gestion de la protection des données)

Quad9: le rôle de la threat intelligence

Quad9 et Switch collaborent pour analyser les menaces qui pèsent sur l'Internet suisse. Cela comprend, entre autres:

- Développement et mise en œuvre d'une stratégie de threat intelligence pour Quad9 et pour Switch (lutte contre l'utilisation abusive des noms de domaine).
- Analyses des principales menaces mensuelles bloquées par Quad9 dans le monde entier et rédaction de rapports réguliers transmis à la communauté de sécurité concernée et aux organisations gouvernementales locales de cybersécurité. Exemples de rapports: Security Awareness Blogpost for Christmas Shopping Season, Trends H1 2024: Cyber Insights et article de blog pour AFRINIC
- Acquisition de nouveaux partenariats de threat intelligence pour Quad9. En 2024, Quad9 a conclu 12 nouveaux partenariats, dont un en Suisse, avec ThreatCat.
  Une liste des partenariats est disponible ici.
- La création d'un «Quad9 Threat Intelligence Product pour Switch CERT». L'objectif de ce projet était de développer une solution pour Switch CERT afin de collecter, d'agréger et d'analyser les données de menace fournies par Quad9 DNS.
- Création d'un tableau de bord Proof of Concept pour le gouvernement suisse. Le tableau de bord montre les principales menaces bloquées par Quad9 au niveau national:



- Comme l'a annoncé le Département fédéral des affaires étrangères (DFAE), Quad9 est devenu le résolveur DNS protecteur pour les ONG et les IGO ayant leur siège en Suisse.

Principales menaces pour le Web suisse

Sur la base des données collectées par Quad9, les campagnes suivantes ont été lancées en 2024 et représentaient un danger pour les internautes suisses:

Campagnes SocGolish

Il s'agit d'une vaste campagne qui vise à distribuer de fausses mises à jour de navigateurs à des internautes peu méfiants. Une fois installées, les fausses mises à jour du navigateur infectent l'ordinateur de la victime avec différents types de malwares, y compris des chevaux de Troie d'accès à distance (RAT).

Dans cette campagne spéciale, blacksaltys.com a été utilisé. Plus de 123 000 requêtes DNS ont été bloquées par Quad9 en Suisse et plus de 7 millions dans le monde.

Phishing CFF

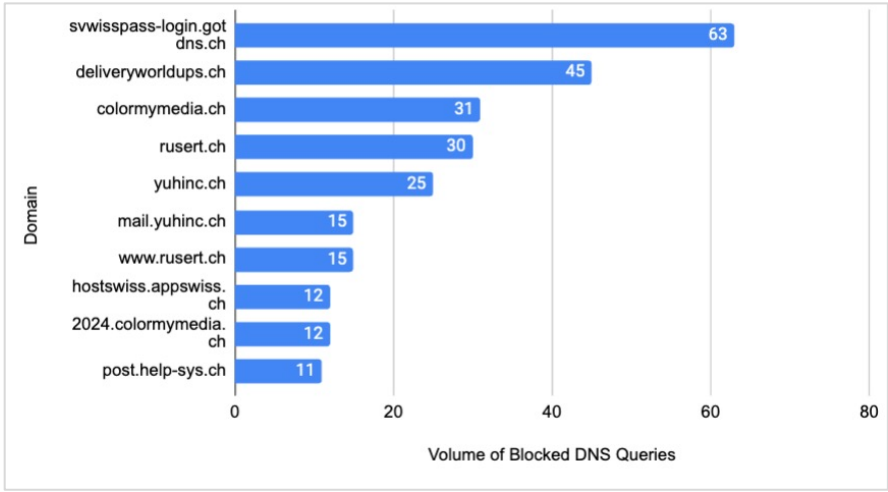
Campagne de phishing qui a poussé les victimes à saisir leurs données SwissPass.

Le nom de domaine utilisé est divinedownload.com. Quad9 a bloqué plus de 2280 requêtes DNS d'utilisateurs suisses.

Phishing la Poste

Campagne de phishing contre la Poste, dans le cadre de laquelle les victimes ont été forcées de communiquer leurs identifiants. Le nom de domaine espace-login.net a été utilisé pour cette campagne. Quad9 a bloqué plus de 2340 requêtes DNS d'utilisateurs suisses.

Les noms de domaine .ch infectés les plus souvent bloqués et transmis par Switch CERT à Quad9 concernaient la campagne contre les utilisateurs de SwissPass et les campagnes contre les expéditeurs (UPS, Deutsche Post) ainsi que les services de messagerie Web.



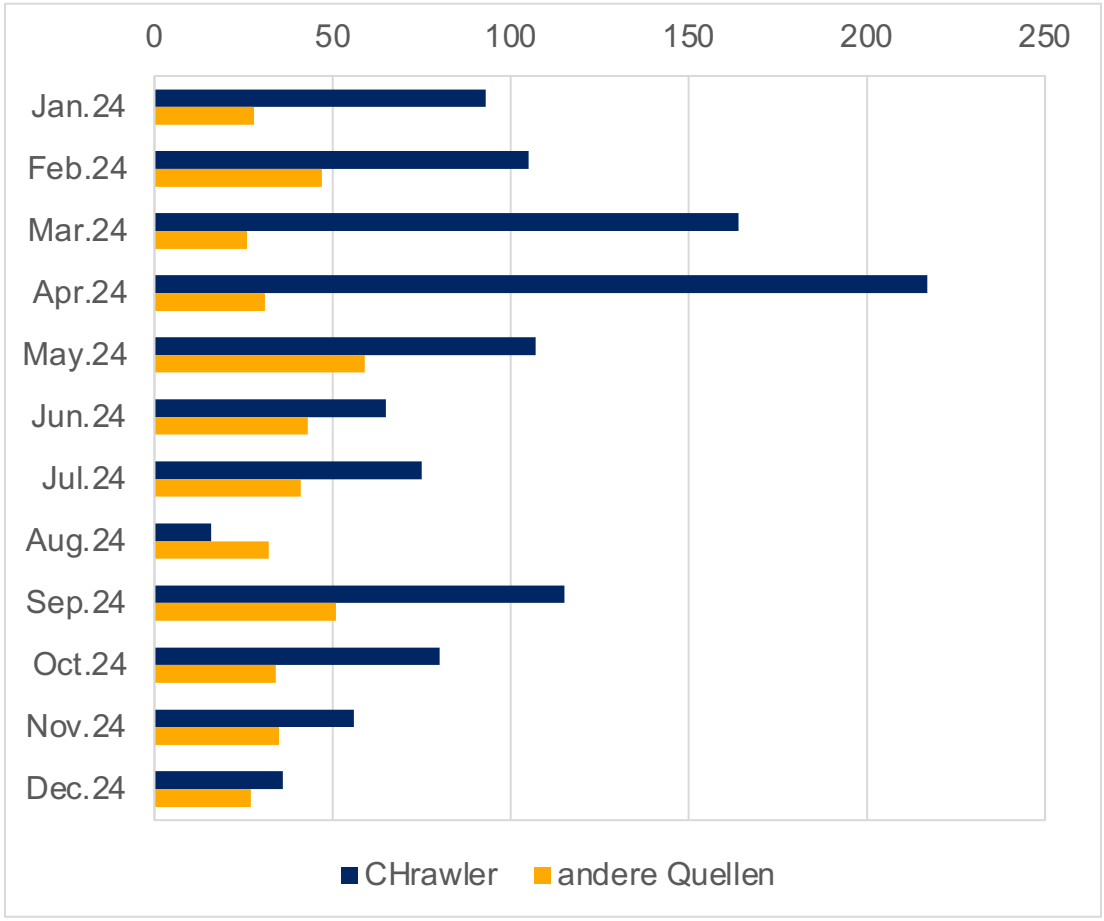
Web crawler

Avec notre Web crawler (CHrawler), qui a été mis en service début 2024, nous analysons régulièrement et systématiquement les ressources accessibles au public dans les zones .ch et .li afin de détecter à temps les noms de domaine compromis ou malveillants et d'éliminer ainsi tout danger pour les internautes. Si nous utilisons notre robot pour détecter des noms de domaine qui font du phishing ou diffusent des malwares, nous pouvons bloquer le nom de domaine après en avoir informé le détenteur et avoir respecté un délai d'attente.

Après près d'un an d'exploitation, il s'avère que nous pouvons régulièrement trouver un nombre considérable de noms de domaine infectés, en particulier par rapport aux chiffres qui nous sont rapportés par ailleurs (voir les statistiques à droite). Au total, nous avons ainsi pu découvrir environ 1200 noms de domaine infectés en 2024.

Ainsi, Switch peut apporter une contribution importante à l'amélioration de la sécurité des zones .ch et .li, non seulement de manière réactive, mais aussi proactive grâce à une recherche autonome. En outre, nous recueillons des informations importantes sur les campagnes et les menaces actuellement actives sur le Web suisse. Voir également «Principales menaces pour le Web suisse», page 32.

Noms de domaine malveillants .ch traités en 2024



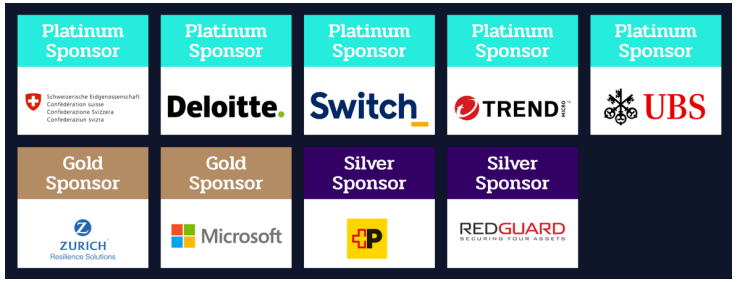
Women in Cyber Switzerland

Malgré la croissance observée ces dernières années dans le domaine cybernétique, on constate que les femmes sont toujours sous-représentées en ce qui concerne la main-d'œuvre mondiale. Cela survient dans le contexte d'une pénurie croissante de main-d'œuvre qualifiée dans ledit domaine. Afin d'aider les entreprises à combler cette lacune, il est important d'enthousiasmer plus de femmes pour ce secteur et de leur offrir les mêmes chances.

«Women in Cyber Switzerland» s'engage pour plus de diversité en organisant le «Women in Cyber Day» annuel, des événements de réseautage locaux et un programme de mentorat.

Switch soutient l'initiative depuis 2019 et est un membre actif du conseil d'administration. Le premier événement de réseautage local a eu lieu en mars chez Switch à Zurich.

https://women-in-cyber.ch



NextGen Hero

De jeunes talents remportent le NextGen Hero Award

Lors de la cérémonie des Digital Economy Awards le 14 novembre 2024, des entreprises, des organisations et des personnalités de différentes catégories ont été récompensées au Hallenstadion de Zurich pour leur contribution unique à la transformation numérique de la Suisse.

Dans la catégorie «NextGen Hero», qui se déroule en collaboration avec Switch, le public présent a sélectionné deux jeunes talents pour leur créativité et leur capacité d'innovation exceptionnelles: Selina Pfyffer et David Cleres.

Qui sont ces stars montantes et quels sont leurs objectifs? Dans cet entretien, elles nous parlent de leurs visions et de la manière dont elles contribuent au progrès numérique de la Suisse.

La cinquième édition des Digital Economy Awards a réuni des centaines de spécialistes de la scène suisse des TIC pour célébrer les talents les plus remarquables et leurs innovations. Les meilleurs d'entre eux ont reçu un prix dans six catégories.

Remise du Digital Economy Award 2024 dans la catégorie «NextGen Hero». De g. à d.: Tom Kleiber, Switch; Claudia Lienert, Switch; David Cleres, GirlsCodeToo; Selina Pfyffer, SeasonCell; Monika Schär, présentation. Photo: Switch

3.
Rapport d’activité – indicateurs statistiques

Switch

Nombre de noms de domaine – évolution 2024

Évolution .ch

En un an, le nombre de noms de domaine .ch a augmenté de plus de 6000.

	2023	2024
Nouveaux enregistrements	294 195	279 916
Suppressions	282 649	303 361
Réactivations*	29 958	29 948
Nombre de domaines au 31 déc.	**2 562 914**	**2 568 952**

Évolution .li

En un an, le nombre de noms de domaine .li a diminué de plus de 1000.

	2023	2024
Nouveaux enregistrements	10 658	9 495
Suppressions	12 218	11 608
Réactivations*	1 699	1 285
Nombre de domaines au 31 déc.	**70 607**	**69 774**

* Noms de domaine supprimés qui ont été réactivés par le registrar au cours de la période de transition de 40 jours.

Service de renseignements – statistiques 2024

Service de renseignements – chiffres

Switch accorde à toute personne justifiant d'un intérêt légitime prépondérant l'accès gratuit aux données personnelles du détenteur ou de la détentrice du nom de domaine concerné contenues dans la base de données RDDS (Whois). Ces statistiques recensent toutes les demandes effectuées durant l'année sous revue via les formulaires du service de renseignements. Le nombre de demandes émanant de particuliers est resté stable par rapport à l'année précédente.

	Particuliers	Autorités
Renseignements fournis	309	73
Renseignements non fournis	54	5
Demandes d'ordre général *	6	0
Total des demandes	**369**	**78**

* Il s'agit ici de demandes concernant les processus, les procédures et les bases légales.

Accès simplifié via RDAP pour .ch et .li

Si une autorité ou une organisation dispose des autorisations nécessaires, elle peut consulter les noms de domaine via RDAP (Registration Data Access Protocol) et obtenir des données personnelles. Le nombre d'autorités a continué à augmenter en 2024, ce qui est également dû à notre meilleure mise en réseau avec les autorités de poursuite pénale. Fin 2022, seules 5 autorités utilisaient le RDAP, contre 17 fin 2024. Les polices cantonales en représentent la plus grande part.

	Demandes
Renseignements fournis	4 203
Renseignements non fournis	368
Total des demandes	**4 571**

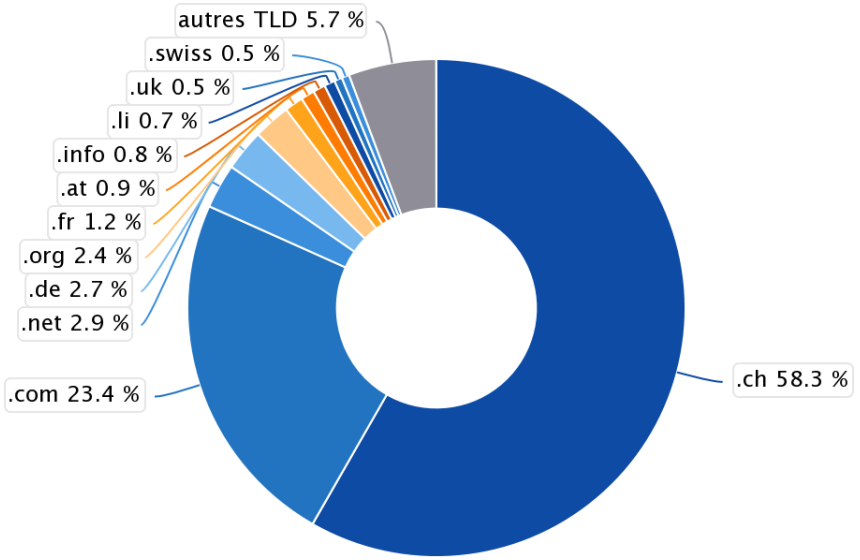
Part de marché de .ch et .li chez les détenteurs et détentrices suisses de noms de domaine

La part de marché du domaine de premier niveau (TLD) **.ch** parmi les détenteurs et détentrices en Suisse est restée pratiquement inchangée entre octobre 2023 et octobre 2024.

La part de marché des TLD génériques **.com/.net/.org** a peu changé, tout comme celle des noms de domaine **.li**.

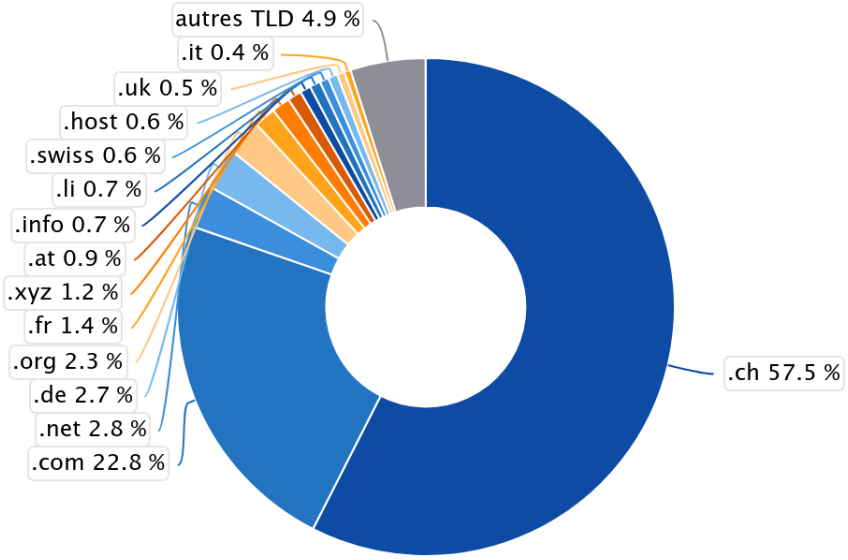
Octobre 2023

Part de marché des différents TLD chez les détenteurs et détentrices de noms de domaine en Suisse. Source: CENTR



Octobre 2024

Part de marché des différents TLD chez les détenteurs et détentrices de noms de domaine en Suisse. Source: CENTR



Programme de résilience DNS – développement en chiffres

DNSSEC

- Pourcentage de noms de domaine .ch avec DNSSEC, état au 1er janvier 2025: 50,4% (1er janvier 2024: 49,1%).
- Taux d'erreurs: Le taux d'erreurs est resté constant à un niveau très bas tout au long de l'année. Taux d'erreurs moyen de tous les noms de domaine DNSSEC: 0,17%, comme en 2023.

DMARC et SPF

- 1er janvier 2025: 20,1% configurés correctement (1er janvier 2024: 4,5%). Chiffres pour les noms de domaine .ch et .li, configuration correcte tant de DMARC que de SPF. Données selon les statistiques du prestataire de services de mesure externe.

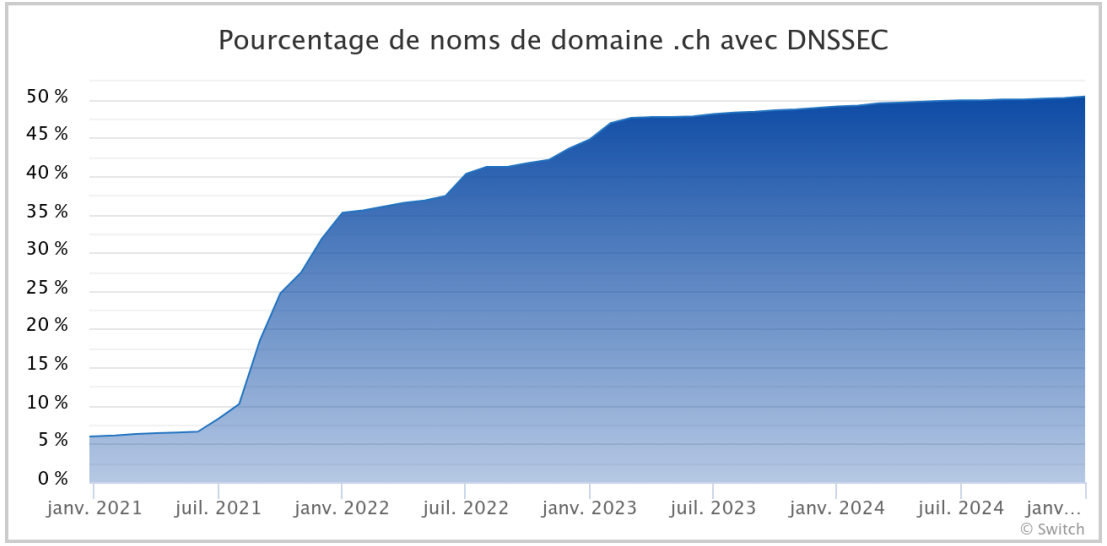
Statistiques DNSSEC chez Switch

Statistiques chez OpenIntel

Calcul du remboursement pour l'année 2024

- Recettes supplémentaires collectées grâce à la différenciation des prix: CHF 1 569 687
- Moins la compensation fixe pour Switch et le prestataire de mesure externe 2024: CHF – 444 907
- Total du remboursement CHF 1 124 790

Les remboursements seront effectués fin février 2025.

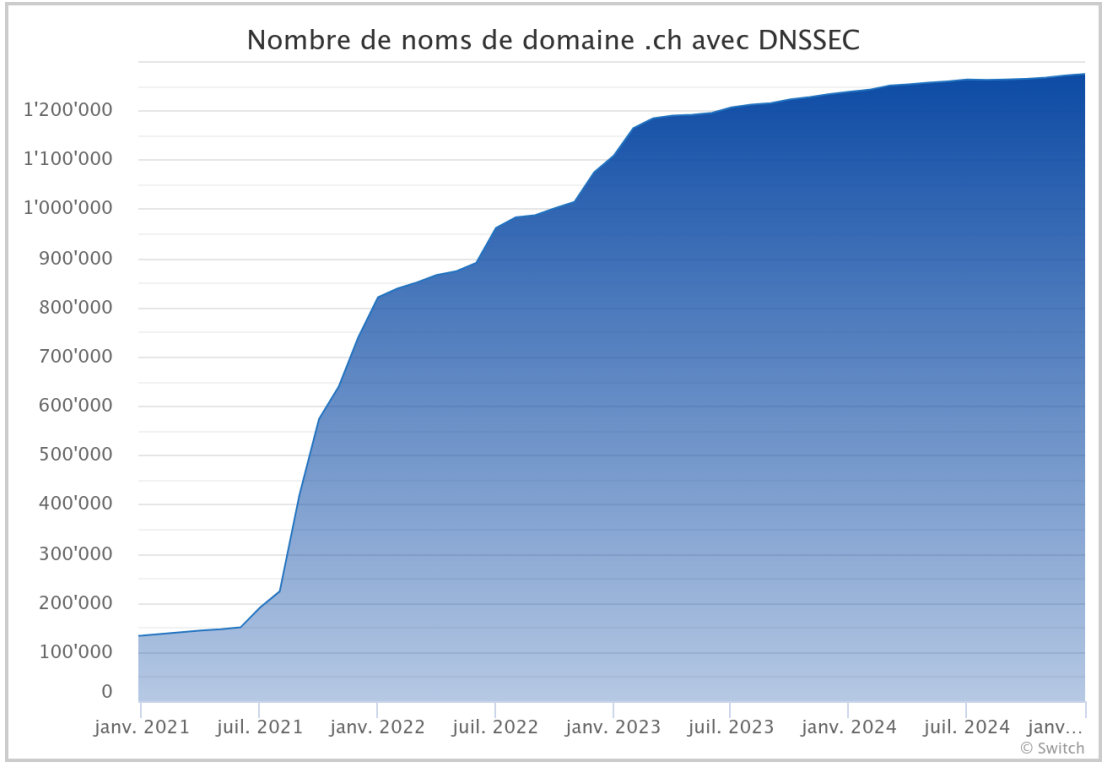


Développement DNSSEC
Nombre de noms de domaine signés

Fin 2024, plus de 1,27 million de noms de domaine .ch ont été signés avec DNSSEC.

Cela correspond à près de 50,4% de tous les noms de domaine .ch avec serveurs de noms, contre 45% fin 2022 et 35% fin 2021. La forte augmentation en 2021 et 2022 est principalement due aux registrars qui ont signé tous les noms de domaine de leurs clients dans le cadre du programme de résilience DNS. Cette croissance s'est ralentie au cours des années suivantes.

Entre-temps, les grands registrars suisses ont signé leurs noms de domaine dans la mesure du possible. Si les noms de domaine ont des serveurs de noms «externes», les registrars n'ont aucune influence sur la signature. Pour les grands registrars à l'étranger, le TLD .ch ne représente qu'une très petite partie de leur activité et l'effort pour la signature n'est pas vraiment rentable pour eux. Il ne faut donc s'attendre qu'à une faible croissance à l'avenir.

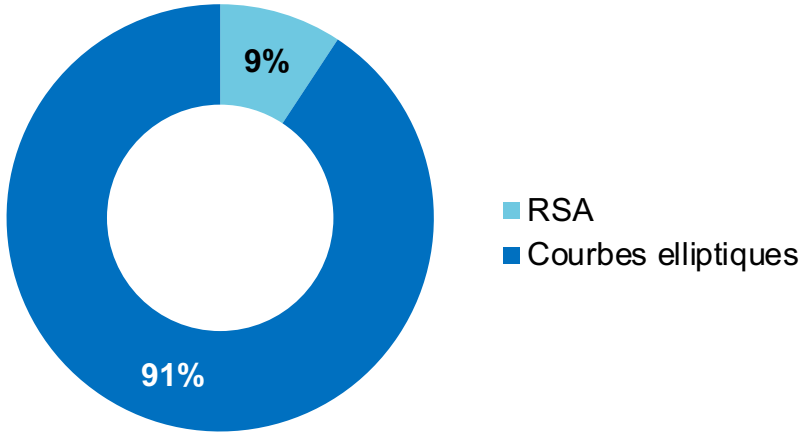


1 273 817 noms de domaine .ch signés avec DNSSEC au 1er janvier 2025

Développement DNSSEC Répartition algorithmes DS

Aujourd'hui, plus de 90% de tous les noms de domaine .ch utilisent l'algorithme 13 (ECDSAP256SHA256) actuellement recommandé.

On constate une légère augmentation de la signature au moyen des courbes d'Edwards (algorithmes EdDSA 15 et 16). Celles-ci ne sont pas ou seulement partiellement prises en charge par les anciens systèmes d'exploitation et ne sont donc, jusqu'à présent, recommandés que de manière limitée.



Signatures DNSSEC utilisées

Algorithme DNSSEC	Nombre	Part
8 – RSASHA256	11 806	9,27%
10 – RSASHA512	86	0,01%
13 – ECDSAP256SHA256	1 153 418	90,55%
14 – ECDSAP384SHA384	150	0,01%
15 – Ed25519	1 929	0,15%
16 – Ed448	123	0,01%

Validation DNSSEC en Suisse

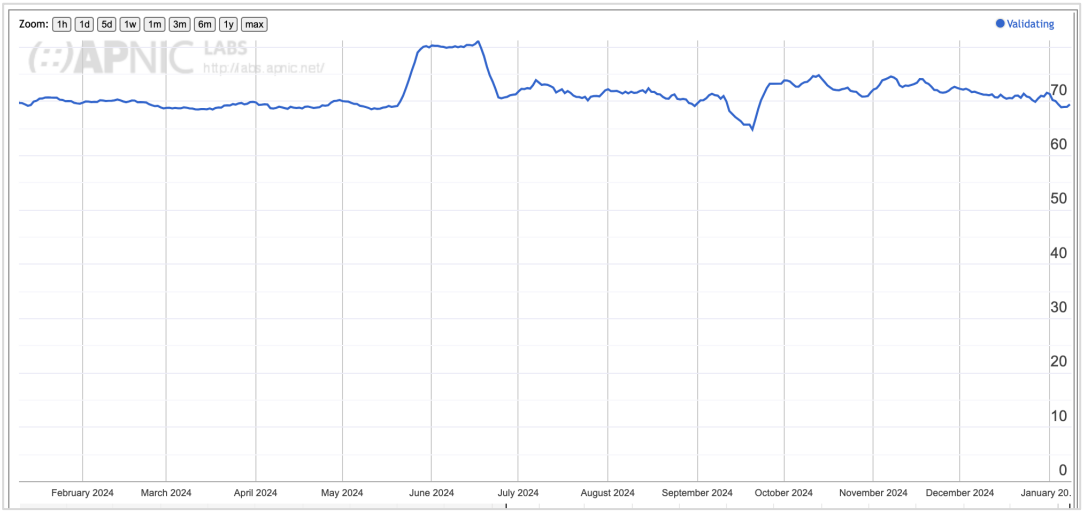
Validation DNSSEC

Pour protéger les utilisatrices et utilisateurs contre l'usurpation de DNS, les noms de domaine doivent, d'une part, être signés et ces signatures doivent, d'autre part, être validées par le résolveur DNS.

Selon les mesures de l'APNIC, le taux de validation DNSSEC sur les résolveurs des FAI suisses est resté constant à environ 70% au cours de l'année dernière.

Page Web: https://stats.labs.apnic.net/dnssec/CH

Validation DNSSEC sur les résolveurs suisses

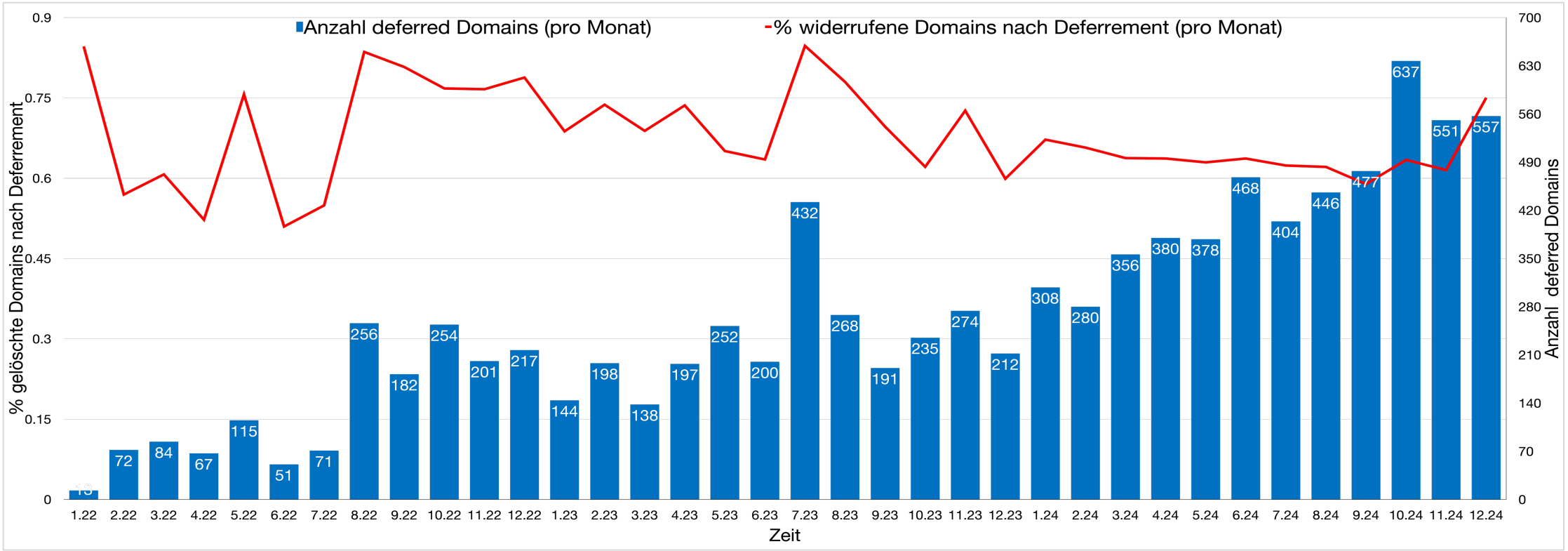


Délégation différée (deferred delegation)

Rétrospective de la délégation différée

L'année dernière, nous avons encore considérablement multiplié par deux le nombre d'enregistrements qui ont été différés (deferred) par de nouveaux durcissements des règles.

Comme on pouvait s'y attendre dans le cadre d'une telle augmentation, la part de noms de domaine rouverts après identification positive du détenteur a légèrement augmenté. Grâce à un élargissement prudent et itératif des critères, cela s'est toutefois produit dans une bien moindre mesure que pour les noms de domaine différés.



Cas de règlement des différends

Sur mandat de l'OFCOM, Switch est chargée d'offrir un service de règlement des différends à un prix avantageux. Pour ce faire, Switch utilise depuis 2004 le service de règlement des différends de l'OMPI (Organisation mondiale de la propriété intellectuelle). L'OMPI exploite un service de règlement des litiges accrédité par l'ICANN pour plus de 70 autres registries.

En 2024, les experts ont pris des décisions pour 13 noms de domaine .ch. La décision des experts est la dernière étape de la procédure. Un nombre un peu moins grand de cas sont déjà terminés avant, par exemple pendant la tentative de conciliation ou en cas d'interruption de la procédure.

Décision de l'OMPI	**2023**	**2024**
Transfert au requérant	11	10
Plainte rejetée	5	3
Nombre de décisions	**16**	**13**

Décisions de l'OMPI (état au 17 février 2025)

	Noms de domaine
Transfert au requérant	girlscancode.ch axashop.ch salonmoulinrouge.ch veka-fenêtre.ch vekafenster.ch floqast.ch elfbar.ch aqara.ch giezemon.ch universalgeneve.ch
Plainte rejetée	carify.ch johntaylor.ch meinl.ch

Évolution registrars

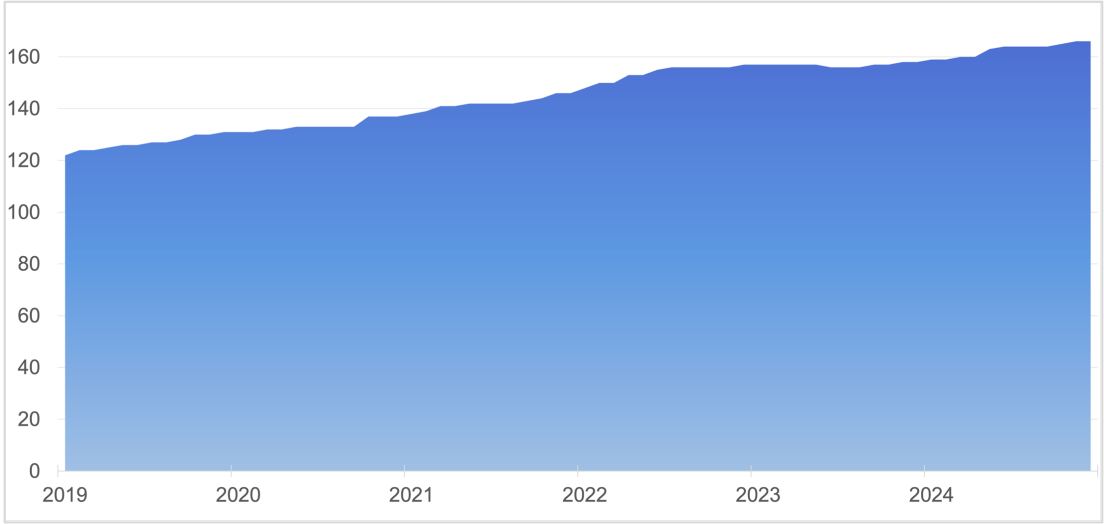
En 2019, le nombre de registrars est passé à 131 et, fin 2020, le registry comptait 137 registrars. En 2021, le nombre de registrars a augmenté de 9 pour atteindre un total de 146.

En 2021, 11 registrars ont d'abord signé un contrat de test pour accéder au système de test. À la suite de la réussite de la phase et du parcours de test, nous avons pu passer ces registrars en mode productif. Le nombre total de registrars reconnus est ainsi passé à 157.

En 2023, nous n'avons pu donner accès au système de production qu'à un registrar supplémentaire et leur nombre est passé à 158.

En 2024, 7 registrars ont été ajoutés, soit un total de 165 à la fin de l'année.

Les huit nouveaux registrars apparus en 2023 et 2024 disposent d'un portefeuille de 8500 noms de domaine, l'un de ces registrars en gérant plus de 7500.



Performance des serveurs de noms

Switch s’appuie sur l’Agreement ICANN pour les exigences relatives aux mesures de performance DNS concernant les temps de réponse aux requêtes DNS: les requêtes à la zone CH doivent recevoir une réponse d’au moins un serveur de noms logique dans un délai de 500 ms (UDP) ou de 1500 ms (TCP).

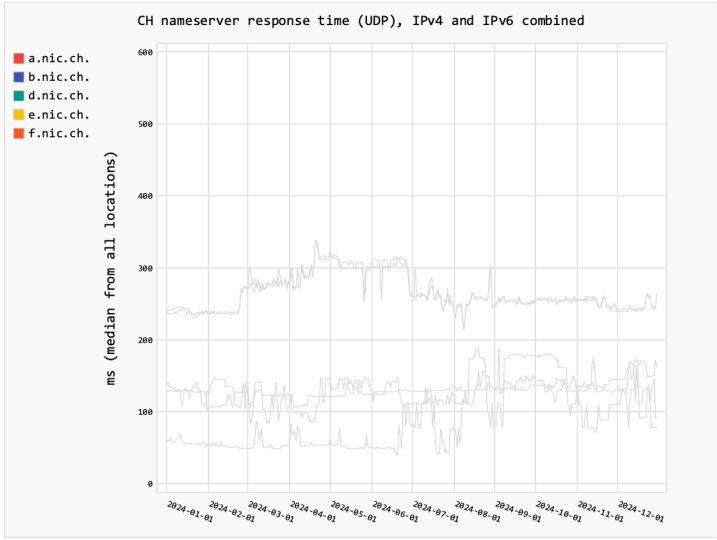
Cette exigence a été respectée en tout temps en 2024.

Les mesures sont effectuées par RIPE et sont accessibles au public.
https://atlas.ripe.net/dnsmon/group/ch

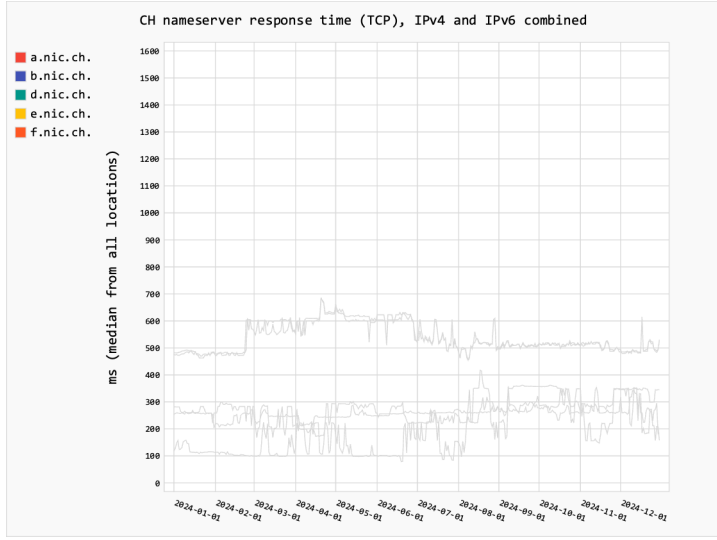
Unicast: a.nic.ch (CH), b.nic.ch (CH)

Anycast: d.nic.ch, e.nic.ch, f.nic.ch

Temps de réponse UDP
Temps de réponse combinés
IPv4 et IPv6



Temps de réponse TCP
Temps de réponse combinés
IPv4 et IPv6



Cybercriminalité 2024

Aspects quantitatifs

Les cas suivants ont été enregistrés et traités au cours de l'année sous revue:

Nombre de cas de malware et de phishing en 2024 observation quantitative

	# cas de malware	# cas de phishing
Notifications reçues	**1 730**	**451**
Soupçon confirmé	**1 392**	**239**
Nombre de noms de domaine bloqués	**656**	**115**
Raison de la levée du blocage: - La durée légale est dépassée - Corrigé après blocage - En cours de traitement à la date de référence	 **83** **402** **3**	 **2** **15** **3**
Noms de domaine révoqués	**170**	**95**

Aspects qualitatifs

Le temps suivant a été nécessaire pour les cas:

Nombre de cas de malware et de phishing en 2024 observation qualitative

	Durée	
Durée du blocage selon l'art. 15 al. 1, 2, 3 de l'ODI, temps de blocage max. 30 jours (720 h)	Durée minimum Moyenne Durée maximum	**0,22 h** **103,74 h** **166,92 h**
Temps de réaction de Switch après notification	Moyenne	**5,13 h**
Temps pour éliminer la menace après la notification au détenteur ou à la détentrice	Moyenne	**86,8 h**

DNS Health Report

Le DNS Health Report vérifie l'accessibilité des serveurs de noms et des noms de domaine en .ch et .li. En cas de problèmes techniques, Switch en informe les exploitants et formule des recommandations pour y remédier. Le DNS Health Report améliore ainsi la fiabilité de l'Internet suisse. Ce qui est vérifié:

- Serveurs de noms: le fonctionnement des serveurs de noms est vérifié pour s'assurer qu'il est conforme aux normes DNS.
- Noms de domaine: il est vérifié si les noms de domaine signés DNSSEC peuvent être résolus par un résolveur récursif validant.

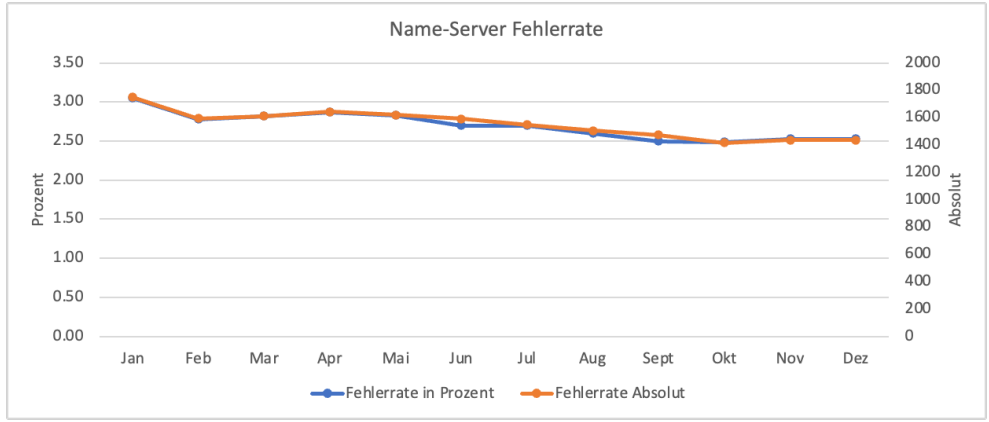
Rapport sur les serveurs de noms

Le taux d'erreur de la mesure de l'accessibilité des serveurs de noms ne diminue que légèrement depuis le début de la mesure, mais constamment. Les mises à jour logicielles en sont la cause la plus probable.

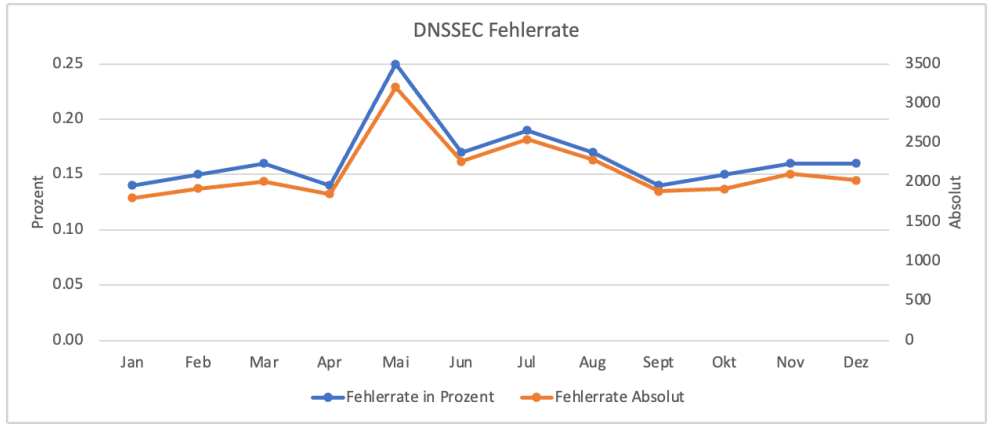
Rapport sur les noms de domaine

Le taux d'erreur de la mesure de l'accessibilité des noms de domaine DNSSEC a atteint un plateau. La plupart des noms de domaine erronés sont des noms de domaine parqués, pour lesquels la motivation à corriger les erreurs est faible.

Taux d'erreur de la mesure de l'accessibilité des serveurs de noms



Taux d'erreur de la mesure de l'accessibilité des noms de domaine



4.

Rapport d’activité – indicateurs économiques

Switch

Indicateurs économiques

La séance du Conseil de fondation du 12 juin 2025 permettra de valider le rapport annuel 2024 de la fondation Switch ainsi que le bilan et le compte de résultat. La publication aura lieu à partir du 13 juin 2025.

Aucun chiffre n’est publié ici, mais il est fait référence aux documents détaillés du rapport annuel 2024 de Switch.

5.
Rapport d’activité – développements

Switch

Rétrospective 2024

Programme de résilience

La différenciation de prix pour les noms de domaine correctement signés avec DNSSEC a été maintenue en 2024. Les incitations financières du programme encouragent la sécurisation cryptographique du DNS ainsi que l'introduction d'autres protocoles sécurisés. En 2024, il s'agissait des normes de sécurité des e-mails DMARC et SPF. Les mesures et le feedback aux registrars se sont déroulés sans accroc. Plus à la page 21

Web crawler pour le registry

Le nouveau Web crawler a été mis en service avec succès début 2024. Cette nouvelle prestation du service d'enregistrement a été rendue nécessaire par le fait qu'il n'y avait plus de messages du NCSC, dont le crawler a été arrêté. Les statistiques à la page 33 montrent les performances impressionnantes du crawler et des processus subséquents liés à la lutte contre l'abus de noms de domaine.

Projet «Domain Abuse 4.0»

Nous avions prévu une durée de deux ans pour que le projet soit terminé fin 2025. Les progrès réalisés en 2024 ont été très satisfaisants. Cela nous permet également de respecter le délai d'achèvement prévu.

Le cadre du contrat avec l'OFCOM stipule clairement que les données dans le cadre de la lutte contre la cybercriminalité doivent être traitées sur des systèmes de Switch. Des recherches approfondies avec des fournisseurs potentiels de logiciels pour certaines parties de l'application ont montré que seul un développement interne peut répondre à cette exigence. L'équipe de développement interne a été renforcée par deux spécialistes externes pour la durée de la mise en œuvre.

Vous trouverez de plus amples informations sur le déroulement du projet à la page 27.

ISMS ISO 27001:2022

Le passage de l'ISMS interne à la nouvelle norme ISO était prévu pour 2024, mais a dû être redéfini.

Nouveautés prévues en 2025

Programme de résilience DNS: mesures IPv6

En 2026, le critère pour le remboursement sera IPv6 pour les serveurs de noms. L'objectif est d'accroître encore la résilience. Switch prépare l'infrastructure de mesure en conséquence. Le Dashboard est également complété afin que les registrars et les hébergeurs puissent vérifier s'ils ont correctement mis en œuvre la configuration conformément aux recommandations de Switch.

Domain Abuse 4.0

Une grande partie de la capacité de développement du service d'enregistrement se concentre sur l'achèvement de la nouvelle infrastructure de lutte contre la cybercriminalité. Cela inclut également la formation des spécialistes qui recevront progressivement de nouveaux outils. Vous trouverez le plan approximatif du projet à la page 28.

Mise à niveau de la base de données

Au deuxième trimestre 2025, la base de données PostgreSQL sera migrée de la version 13 à la version 16. Le cœur de l'application d'enregistrement sera ainsi renouvelé. Une préparation minutieuse est une condition importante. Nous nous appuyons également sur des experts externes en matière de bases de données.

ISMS ISO 27001:2022

L'audit de deux jours selon la norme 2022 aura lieu les 10 et 11 septembre 2025. D'ici là, tous les documents et processus du système de gestion de la sécurité de l'information ISMS devront être adaptés.

Nouveautés prévues en 2025

Délégation différée et Machine Learning

Des règles qui recherchent certains modèles (patterns) et procèdent ensuite à une pondération de ces résultats déterminent si un nom de domaine entre ou non dans le processus de délégation différée lors du nouvel enregistrement. Cela peut être vérifié de manière transparente dans tous les cas.

Switch développe un nouvel algorithme qui utilise le Machine Learning. Les patterns restent primordiaux. La pondération devient toutefois plus dynamique. Le système est entraîné avec des noms de domaine qui sont confirmés comme abusifs ou qui sont enregistrés sans utilisation abusive depuis longtemps. Les services d'enregistrement de Belgique et des Pays-Bas utilisent déjà un tel outil et partagent leur expérience.

Le passage à ce nouveau système n'aura vraisemblablement pas lieu en 2025. Il s'agit tout d'abord d'acquérir des connaissances et de vérifier le concept.

Domain scanner pour CDS

En 2025, il est prévu de renouveler l'infrastructure pour la gestion automatique des enregistrements DS de DNSSEC. Le scanner, qui parcourt quotidiennement toute la zone à la recherche d'enregistrements CDS (RFC8078), gagne en efficacité grâce à un algorithme de recherche amélioré. Les enregistrements CDS sont ainsi trouvés et traités plus rapidement. De plus, des travaux préparatoires sont en cours pour lancer à l'avenir une recherche de noms de domaine individuels à n'importe quel moment, de sorte qu'il n'est pas nécessaire d'attendre la prochaine recherche quotidienne.

L'infrastructure de numérisation rénovée aussi crée les bases pour traiter à l'avenir, en plus des données DNSSEC, les enregistrements CSYNC (RFC7344) qui permettent la gestion automatisée des informations du serveur de noms.

RPP – RESTful Provisioning Protocol

D’EPP à RPP

L’Extensible Provisioning Protocol (EPP) a été normalisé en 2009 et a simplifié la communication entre les services d’enregistrement et les registrars. Avant l’introduction de l’EPP, les différents registries n’avaient pas d’interfaces uniformes pour l’enregistrement et la gestion des noms de domaine.

Bien que l’EPP continue de rendre de bons services au secteur, les progrès réalisés dans les outils de développement et d’intégration ainsi que dans les processus opérationnels et les technologies utilisées suscitent le désir d’un nouveau protocole de provisioning.

À quoi pourrait ressembler un protocole moderne?

Une approche évidente consiste à utiliser l’architecture REST et le format d’échange de données JSON. Un tel design peut tirer parti d’une architecture sans état et de solutions largement répandues telles que OpenAPI, des outils de test et de génération de code, des passerelles API, des serveurs d’autorisation, des répartiteurs de charge, etc.

L’architecture REST doit permettre une intégration plus simple entre les services d’enregistrement et les registrars. L’introduction réussie de RDAP a démontré l’utilité de ce type d’architecture. L’intégration et l’efficacité peuvent être améliorées sans renoncer à la standardisation.

Le nouveau protocole s’appellera RPP (RESTful Provisioning Protocol).

- Il doit servir de complément moderne à l’EPP.
- Un nouveau groupe de travail sur RPP est en cours de création au sein de l’IETF (Internet Engineering Task Force).
- L’objectif de ce groupe de travail est la spécification et la standardisation de RPP.
- Switch suit l’évolution actuelle et apporte son expertise en matière d’EPP et de REST.

Article sur RPP chez DENIC

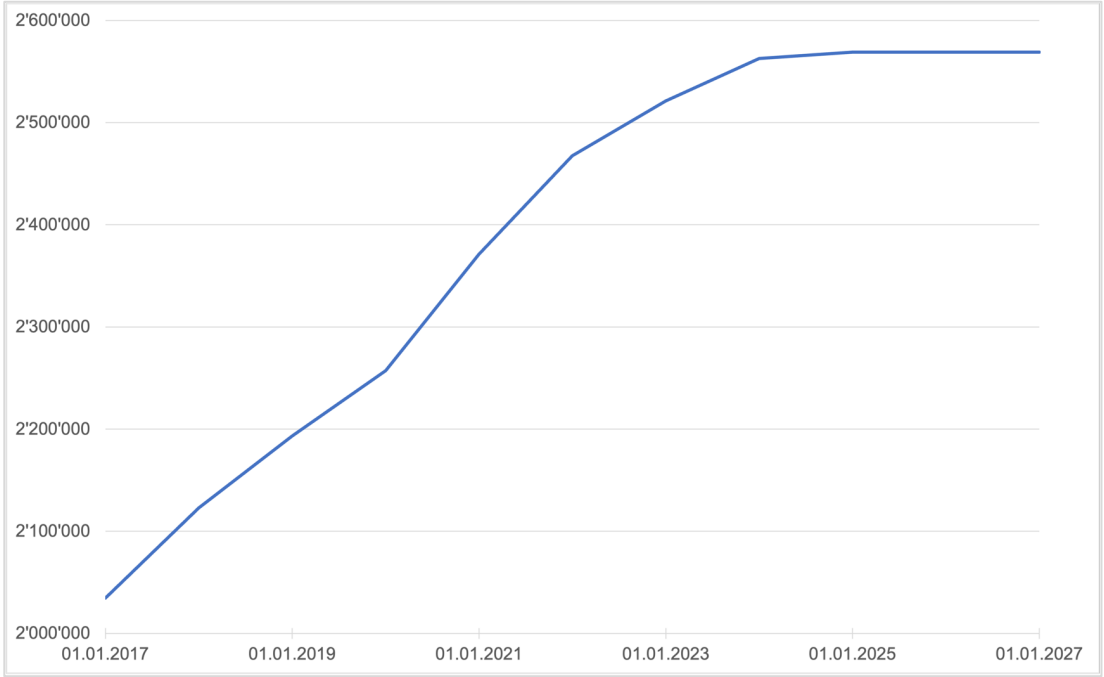
Prévisions de croissance des noms de domaine .ch

Les années 2018 et 2019 ont montré une augmentation, légèrement inférieure d'une année à l'autre. En 2020, la poussée de la numérisation due à la pandémie et les initiatives marketing des hébergeurs Web ont entraîné une augmentation de la demande et donc une croissance de 4,8%. En 2021, la croissance a diminué pour atteindre 3,9%, mais est restée plus élevée qu'avant la pandémie.

Pour 2022, le service d'enregistrement a encore enregistré une croissance de 2,1%. La poussée de la numérisation a donc duré deux ans et entraîné une augmentation inattendue d'environ 100 000 noms de domaine.

En 2023, l'augmentation a été de près de 40 000 noms de domaine. Cela correspond à 1,6% et n'atteint pas nos prévisions de 1,8%.

Pour 2024, nous avions encore une croissance de 6000 noms de domaine. Nos prévisions pour l'année 2025 tablent sur une croissance nulle.



Switch
Werdstrasse 2
Case postale
CH-8021 Zurich

Tél. +41 44 268 15 15
www.switch.ch
info@switch.ch

Switch