

Switch

Resoconto 2023

del registry .ch

Indice

Editoriale 4

Attività operativa 5

Lotta alla criminalità informatica
Misure in caso di sospetto abuso
Security Awareness
Community Events
Evento LEO
Domain pulse 2023
Programma di resilienza DNS
DNS: sedi Anycast e generazione della zona
Ricertificazione ISMS

Novità 22

Domain Abuse 4.0
Fondazione dell'European TLD ISAC
Web crawler
Nuova legge sulla protezione dei dati
Quad9: il ruolo della Threat Intelligence
Principali minacce per il web svizzero
Nuova sede a Losanna
IPv6 Evangelist
Sondaggio clientela registrar

Statistiche 33

Portafoglio nomi a dominio
Servizio informazioni
Quota di mercato di .ch e .li
Programma di resilienza DNS
Evoluzione di DNSSEC
Validazione DNSSEC in Svizzera
Deferred Delegation
Composizione delle controversie
Evoluzione dei registrar
Performance dei name server
Criminalità informatica
DNS Health Report
DAAR - Domain Abuse Activity Reporting

Dati economici 51

Dati economici 2023

Sviluppi 53

Uno sguardo al 2023
Prospettive strategiche e obiettivi
Novità pianificate 2024
Previsione di crescita per i nomi a dominio .ch



*Facciamo tutto il possibile
per assicurare il futuro
del nostro ecosistema
digitale.*

Urs Eppenberger
Head of Registry, Switch

Piena forza innovativa nella lotta alla criminalità informatica

Urs Eppenberger, Head of Registry

Il costante impegno di Switch nella lotta alla criminalità informatica ha portato alla progettazione di «Domain Abuse 4.0». L'obiettivo del progetto è assicurare il futuro del nostro ecosistema digitale. Le fondamenta della nostra lotta alla criminalità informatica devono essere ridefinite. I processi vengono ottimizzati e l'intera infrastruttura tecnica viene rinnovata. Una descrizione del progetto è riportata a pagina 23.

Mentre in Svizzera l'azione penale spetta in linea di principio alle autorità competenti, Switch occupa una posizione particolare. Switch gestisce infatti un proprio CERT (Computer Emergency Response Team) e offre servizi di sicurezza all'avanguardia alle università svizzere e all'economia. Grazie alla collaborazione con altri CERT e alla stretta cooperazione con le autorità incaricate del perseguimento penale, Switch diventa un'istanza agile e capace di gestire autonomamente il flusso di casi di malware e phishing in modo particolarmente efficiente ed efficace. L'UFCOM se ne è reso conto presto, ha creato le basi legali necessarie e ha sancito il relativo incarico nel contratto con Switch.

La lotta alla criminalità informatica presso Switch è simile a un macchinario altamente complesso in cui specialiste e specialisti di discipline diverse lavorano insieme, creano reti con altri attori in questo settore e collegano tra loro varie componenti informatiche.

Gli utenti svizzeri non hanno mai avuto una vita facile: si assicurano il proprio nome a dominio presso un registrar e gestiscono il proprio sito web presso un provider di hosting. Questi servizi sono disponibili a prezzi interessanti. Tuttavia, gli sforzi necessari dietro le quinte per garantire il funzionamento sicuro e stabile di Internet nel suo complesso e di ogni singolo nome a dominio sono in gran parte sconosciuti. Tali sforzi richiedono una collaborazione collaudata e consolidata tra hosting provider, registrar, Switch e le autorità preposte al perseguimento penale.

Chiunque si occupi della lotta contro la criminalità informatica conosce l'importanza e la necessità di questo lavoro. Ecco perché noi di Switch abbiamo deciso di intensificare ulteriormente i nostri sforzi. La registrazione e la gestione dei nomi a dominio, come compito principale del registry, sono organizzate in modo così efficiente che è possibile concentrare tutta la forza innovativa nella lotta contro la criminalità informatica. In questo modo continueranno a essere garantite la massima sicurezza e stabilità per tutti gli utenti di Internet.

1.

Rapporto d'attività operativa

Lotta alla criminalità informatica

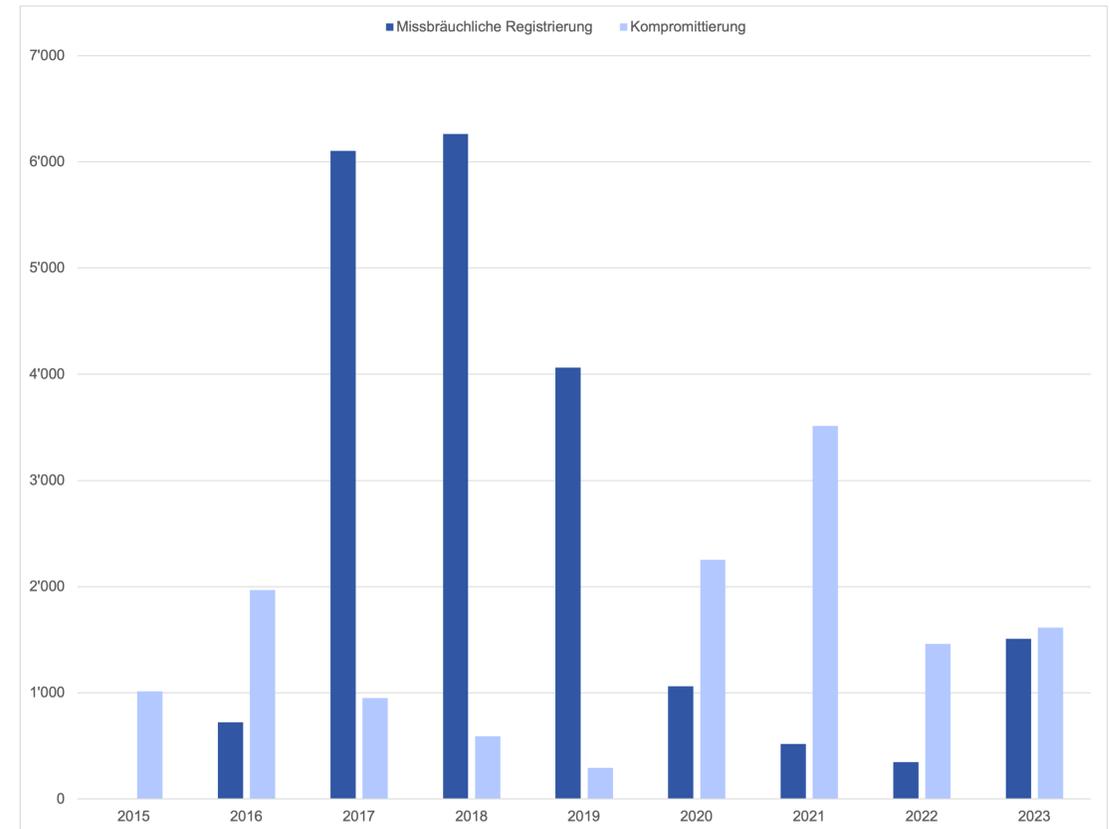
Siti web compromessi

Il numero di siti web compromessi che sono stati manipolati per scopi di phishing e malware è rimasto all'incirca costante rispetto all'anno precedente.

Registrazione abusiva

Il numero di nomi a dominio per cui si sospetta una registrazione abusiva, invece, è aumentato. Uno dei motivi è che la Fedpol ha inviato più richieste ai sensi dell'art. 15 tramite il suo progetto «SWITCHoff».

Sito web: <https://saferinternet.ch>



Misure in caso di sospetto abuso

Richieste di autorità riconosciute – ODIn 15.1

Nel 2023, le autorità accreditate hanno inviato un totale di 426 richieste di blocco immediato (tecnico/amministrativo) di nomi a dominio riguardanti phishing o malware secondo l'art. 15.1 dell'ODIn.

| Richieste | Conseguenza | 2023 |
|----------------|---------------------------|------------|
| Senza risposta | Nomi a dominio cancellati | 410 |
| Con risposta | Nomi a dominio riattivati | 16 |
| Totale | | 426 |

Tutti gli enti riconosciuti dall'UFCOM sono elencati sul seguente sito web: [Enti riconosciuti](#)

Assistenza amministrativa – ODIn 16.3

L'istanza di un'autorità svizzera intervenuta nel proprio ambito di competenza ha comportato l'invio di 1'084 richieste per un indirizzo postale svizzero secondo l'art. 16.3 dell'ODIn.

| Richieste | Conseguenza | 2023 |
|----------------|---------------------------|--------------|
| Senza risposta | Nomi a dominio cancellati | 964 |
| Con risposta | Nomi a dominio riattivati | 120 |
| Totale | | 1'084 |

Security Awareness – iBarry e SISA

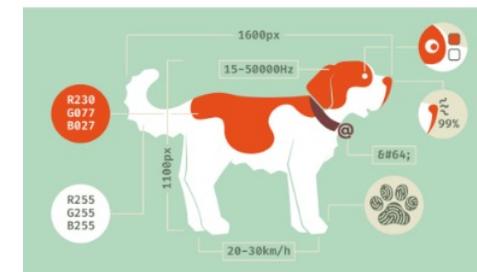
In collaborazione con SISA, Switch sostiene la sensibilizzazione della popolazione svizzera. Con tre nuove campagne informative (fake news, protezione dei dati, VPN), iBarry.ch informa e offre al contempo orientamento e supporto in caso di dubbi e domande relative alla sicurezza su Internet.

<https://checkawebsite.ibarry.ch>

<https://www.ibarry.ch>

Al fine di ottimizzare l'offerta per la popolazione svizzera e posizionare meglio la piattaforma iBarry, SISA ha partecipato anche quest'anno al sondaggio degli utenti svizzeri di Internet.

<https://internet-sicherheit.ch>



Security Awareness Day

Il 26 ottobre 2023, Switch ha organizzato per la sesta volta il Swiss Security Awareness Day. Quest'anno la conferenza, in costante crescita, si è svolta con iBarry come partner. Tra le interessanti presentazioni, i circa 120 partecipanti hanno potuto fare rete con altre esperte ed esperti in diverse pause di networking.

Anche questa volta il programma si prefiggeva di migliorare la comprensione della Security Awareness nella Switch-Community, approfittando al tempo stesso dell'occasione per trasmettere nuove idee e stimolare lo scambio.

Tutti gli interventi sono online: <https://swit.ch/ssad2023-recordings>



Security Awareness Adventures

The Switch Security Awareness Adventures

«Hack The Hacker – l'Escape Room» è stata la prima di tre Security Awareness Adventures di Switch, seguita da «Track The Hacker – la caccia al tesoro» e «Piece of Cake – il gioco di ruolo». Le avventure continuano a godere di grande popolarità: nel 2023, Switch ha tenuto 40 sessioni ludiche di formazione sulla sicurezza e ha aiutato tre organizzazioni a realizzare le proprie sessioni.

Anche 12 collaboratori dell'UFCOM sono riusciti ad hackerare l'hacker.

Pagina web: <https://swit.ch/security-awareness-adventures>



Security Awareness – Podcast

Podcast: Security Awareness Insider

A dicembre 2023 è uscita la 38a puntata del podcast «Security Awareness Insider» (in tedesco).

Qui Katja Dörlemann (Switch) e Marcus Beyer (Swisscom) non solo parlano della sensibilizzazione dei collaboratori in tema di sicurezza, nuove e creative tecnologie, tool e approcci di formazione, ma danno anche uno sguardo al programma di Security Awareness di aziende e organizzazioni e a molto altro ancora.

Dall'inizio il podcast è già stato scaricato 17'000 volte, per ogni nuova puntata si registrano in media 400 download.

Disponibile su Spotify o al seguente link:

<https://www.securityawarenessinsider.ch>



Community – Swiss Web Security Day

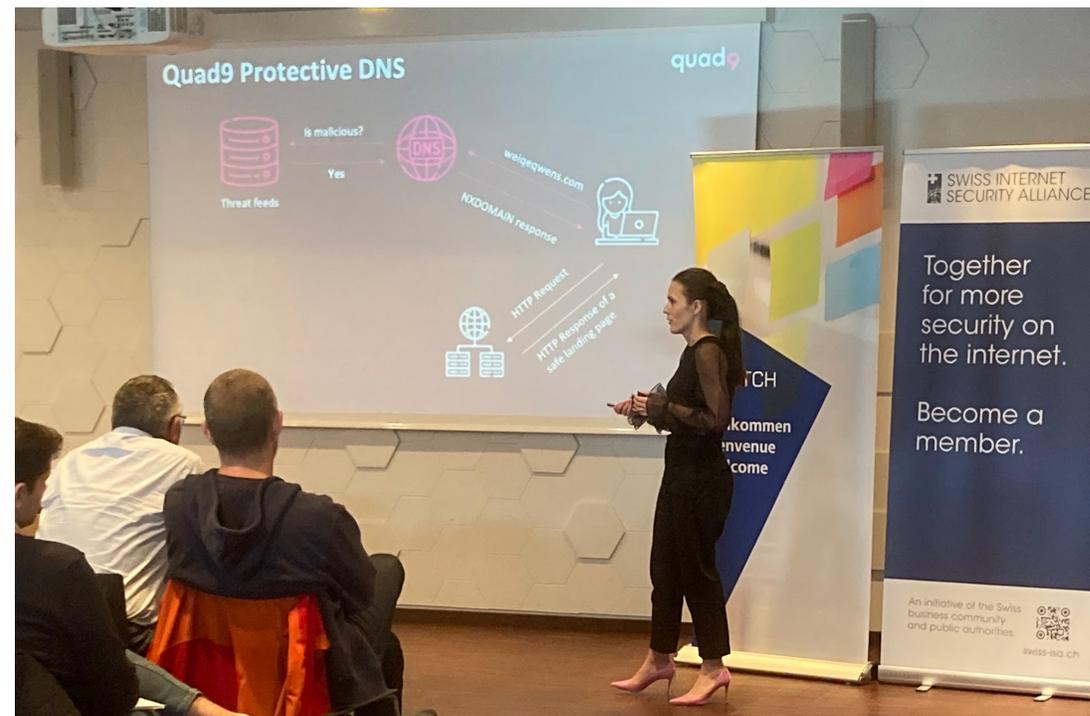
Il 17 ottobre 2023, Switch ha organizzato il Swiss Web Security Day a Berna insieme a SISA e Swico, parallelamente all'evento LEO con le autorità svizzere di perseguimento penale. L'evento è stato un vero successo grazie alla presenza di 73 partecipanti dalla Svizzera e dall'estero, ottenendo riscontri molto positivi dai partecipanti.

In mattinata si sono svolte presentazioni sulle linee guida per la comunicazione sicura tramite e-mail, Medicrime, la gestione delle vulnerabilità in Svizzera, le minacce per gli utenti svizzeri di Internet e un aggiornamento relativo alla revisione dell'Ordinanza sui domini Internet (ODIn). Il pomeriggio è stato dedicato a workshop e discussioni in piccoli gruppi, seguite da un aperitivo.

Questa volta l'evento non si è svolto più in modalità ibrida, ma in presenza a Berna.

Pagina web: <https://swsd2023.events.switch.ch>

Il Swiss Web Security Day si svolgerà di nuovo nel 2024: 29 ottobre 2024, Welle 7, Berna.



Community – Corso ModSecurity

ModSecurity è un firewall di applicazioni web open source molto popolare e potente. I firewall di applicazioni web rappresentano un elemento importante per la protezione di un'applicazione web e sono quindi interessanti per hosting provider, registrar, ma anche in generale per qualsiasi gestore di un'applicazione web.

Per offrire un valore aggiunto alla nostra community, il 15 e 16 marzo 2023 Switch ha organizzato un corso introduttivo presso la sede Switch di Zurigo in collaborazione con l'esperto di ModSecurity di fama mondiale Dr. Christian Folini di Netnea. Switch ha sfruttato i suoi buoni rapporti con la community per attirare l'attenzione sul corso, ha messo a disposizione i locali e ha sponsorizzato biglietti scontati per registrar e clienti di Switch.

Alla fine, al corso di Zurigo ha partecipato un variegato mix di registrar, hosting provider e collaboratori di scuole universitarie.

Nel 2024 è prevista una nuova edizione.

modsecurity
Open Source Web Application Firewall

netnea

Evento LEO

Cooperazione con le autorità di perseguimento penale

Gruppo target

Per consolidare la collaborazione con le autorità, quest'anno Switch ha organizzato la terza edizione dell'evento LEO. LEO sta per «Law Enforcement Organizations».

Il 17 ottobre 2023 la Law Enforcement Community si è riunita a Berna. All'evento LEO erano presenti 63 persone. Molte avevano partecipato già l'anno precedente e hanno portato con sé i colleghi interessati. Ogni anno si registra un aumento.

La distribuzione tra le regioni è stata molto equilibrata e gli interventi si sono svolti nelle lingue nazionali e in inglese. I partecipanti erano rappresentanti di autorità come le polizie cantonali, le procure cantonali e la polizia nazionale del Liechtenstein. Ma c'erano anche enti come Swissmedic, Seco e l'UFCOM.



Argomenti

Sono stati affrontati diversi argomenti. L'attenzione si è concentrata sulla collaborazione all'interno della community per prevenire la criminalità informatica. Sono stati presentati diversi casi che è stato possibile risolvere con successo ed efficienza grazie alla collaborazione dei partner della community.

È stato presentato un caso di studio finlandese che fornisce spunti su come risolvere i casi, anche quando all'inizio sembrano molto difficili. Sono state discusse le «Lessons Learned» sulle richieste secondo l'ODIn a Switch con le loro possibili insidie e i partecipanti dell'UFCOM hanno affrontato le domande della community.

Risonanza

L'evento ha riscosso un grande successo. I partecipanti hanno parlato degli sviluppi e dei progetti attualmente in corso nel settore degli abusi di dominio e della criminalità informatica. Si è inoltre discusso di processi e interfacce che possono rendere più semplice la collaborazione. Il confronto all'interno della collaborazione è cresciuto molto. I partecipanti auspicano un altro evento nel 2024.

Domain pulse 2023

In occasione del Domain pulse di quest'anno, il 6 e 7 febbraio 2023 esperti del settore provenienti principalmente da Svizzera, Germania e Austria si sono incontrati per discutere della sicurezza e della stabilità di Internet.

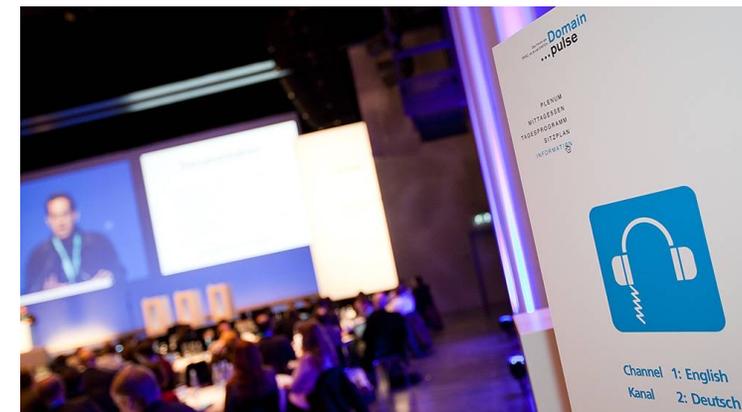
Circa 250 partecipanti provenienti da uffici di registrazione, registrar, hosting provider, uffici federali e altri esperti hanno accolto l'invito a Winterthur.

Con il titolo «Infrastruttura critica Internet: tutelare la sovranità e proteggere dagli abusi», hanno discusso in merito alle attuali sfide del settore Internet.

Il tema centrale è stato il modo in cui la politica e le organizzazioni di gestione di infrastrutture critiche mantengono la sovranità su Internet in tempi di conflitti internazionali, proteggendolo dagli attacchi e rendendolo più affidabile.

La sala conferenze barocca è stata una delizia per gli occhi di molti partecipanti e il tempo dedicato al networking è stato molto apprezzato.

Non vediamo l'ora di tornare a ospitare l'evento Domain pulse nel 2026.



Programma di resilienza DNS

50%

Al 1° gennaio 2024 già quasi il 50% di tutti i nomi a dominio .ch era autenticato.

Programma di resilienza DNS

Capacità di resistenza per i nomi a dominio .ch

Il programma di resilienza DNS promuove l'introduzione e l'applicazione di standard di sicurezza aperti per i nomi a dominio .ch e .li. L'impiego di tali standard è determinante per la capacità di resistere alle minacce informatiche (resilienza). Il programma si basa su un sistema di incentivi finanziari e dura dal 2022 al 2026.

L'obiettivo principale è incentivare l'autenticazione dei nomi a dominio con DNSSEC. Per tutta la durata del programma, in caso di nomi a dominio non autenticati o non autenticati correttamente, ai registrar verrà applicato un supplemento sul prezzo.

Il «DNSSEC Advisory Board» stabilisce gli standard da promuovere. In questo organo sono rappresentati l'UFCOM, un delegato dei registrar e Switch.

Per il 2024 saranno incluse nel programma anche le tecnologie per la sicurezza delle e-mail DMARC e SPF. Per il rimborso delle entrate supplementari non è determinante solo DNSSEC, ma anche l'implementazione di DMARC e SPF.

L'Advisory Board ha già stabilito che, in aggiunta al DNSSEC, saranno promossi DANE nel 2025 e IPv6 nel 2026. In questo modo i registrar hanno tempo a sufficienza per frequentare i corsi di perfezionamento offerti da Switch e pianificare le misure tecniche.

Misurazioni per il controllo della qualità

Come nel caso di DNSSEC, anche per la misurazione delle altre tecnologie di sicurezza si ricorre al fornitore esterno di servizi di misurazione OpenIntel. Le misurazioni verificano per tutti i nomi a dominio .ch e .li con name server se i criteri definiti da Switch per il programma sono soddisfatti e lo comunicano quotidianamente a Switch. In caso di configurazioni errate, i registrar ricevono da noi i cosiddetti Error Report.

Programma di resilienza DNS

Anche nel suo secondo anno di attività ci siamo occupati costantemente, oltre che del funzionamento, dell'ulteriore sviluppo del programma di resilienza.

Sviluppi 2023

- Rimborsi per il 2022 ai registrar aventi diritto sotto forma di accrediti (fine gennaio 2023).
- Implementazione delle misurazioni di DMARC e SPF, che saranno rilevanti nel 2024.
- Da settembre 2023 invio dei nuovi Error Report per DMARC/SPF ai registrar. Anche se il criterio sarà determinante solo nel 2024, i registrar avranno così la possibilità di prepararsi.
- Estensione della dashboard per DMARC/SPF presso il fornitore esterno di servizi di misurazione [OpenIntel](#) (screenshot a destra).
- Informazioni continue ai registrar, risposta alle loro richieste, assistenza.

- Due nuovi report che consentono al registrar interessato di comprendere la valutazione dei propri nomi a dominio.
- Training su DNSSEC e DANE a Zurigo e Losanna a ottobre 2023.

The screenshot displays the SWITCH DNS Resilience Dashboard for the domain saferinternet.ch on 2023-12-31. The dashboard is divided into two main sections: DNSSEC Status and DMARC/SPF Status. Both sections show a large green checkmark in a circle, indicating a 'Well done!' status. Below each checkmark, a message states: 'This domain name fulfills the technical DNSSEC requirements of the DNS resilience programme. No action required.' and 'This domain name fulfills the technical DMARC/SPF requirements of the DNS resilience programme. No action required.' respectively. At the bottom of each section, there are two rows of status indicators: 'Evaluation Report' and 'Measurement data available', both marked with green checkmarks. The DMARC/SPF section also includes a 'DMARC record present' indicator, also marked with a green checkmark. The dashboard header includes 'SWITCH DNS Resilience Dashboard' and navigation links for 'Dashboard', 'Statistics', and 'About'.

DNS: sedi Anycast e generazione della zona

Sedi Anycast

Nel 2023 i nostri partner di hosting DNS Anycast hanno aggiunto diverse sedi in Svizzera e all'estero nelle quali viene predisposta la zona DNS tramite Anycast. Ad esempio, da gennaio 2023 è attivo un Point of Presence a Ginevra.

Generazione della zona

L'infrastruttura per la generazione e la distribuzione della zona è stata completamente rinnovata nel 2023. Gli «Hidden Primary Server» che creano la zona e generano le autenticazioni DNSSEC hanno ricevuto un nuovo hardware.

A causa dell'elevata percentuale di nomi a dominio autenticati DNSSEC e dei nuovi requisiti in seguito alla pubblicazione della zona .CH nel 2020, è stato modificato anche il metodo di creazione delle autenticazioni DNSSEC per i nomi inesistenti:
Finora: «NSEC3 con opt-out»
Novità: «NSEC»



Ricertificazione ISMS

Dal 5 al 7 settembre 2023 si è svolta la ricertificazione del sistema di gestione della sicurezza dell'informazione ISMS secondo la norma ISO 27001:2013.

Per tre giorni, l'auditor si è fatto un'idea di tutti gli aspetti dell'ISMS presso Switch secondo le disposizioni per una ricertificazione. Switch ha superato l'audit con successo senza anomalie o osservazioni.

L'auditor ha fissato sette consigli su come Switch può migliorare concretamente l'ISMS. Queste raccomandazioni confluiscono nel processo di miglioramento continuo CIP dell'ISMS.

La relazione dell'auditor esprime un'impressione generale positiva, conclusa con la seguente osservazione: «C'è un alto livello di impegno da parte della Direzione generale e una grande comprensione per quanto riguarda la sicurezza delle informazioni tra tutti i collaboratori intervistati. Uno dei punti di forza di Switch è rappresentato dal miglioramento continuo e dalle elevate conoscenze specialistiche dei collaboratori a tutti i livelli.»

ZERTIFIKAT

Nr. 860-ISMS-23

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 1.4 vom 14.10.2021 | 05/12/2017 | 09/10/2023 | 05/12/2026 |



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.

«Uno dei punti di forza di Switch è rappresentato dal miglioramento continuo e dalle elevate conoscenze specialistiche dei collaboratori a tutti i livelli.»

ISO 27001 Relazione di audit

2.

Rapporto d'attività – Novità

Domain Abuse 4.0

Esigenze crescenti

Con un convincente team di esperti e il supporto di soluzioni software sviluppate internamente, Switch combatte da anni l'abuso dei nomi a dominio nella rete Internet svizzera. I criminali informatici diventano sempre più astuti e, di conseguenza, crescono le richieste nei confronti degli esperti e delle soluzioni software.

La sfida della soluzione software attuale

Il codebase della soluzione software attuale per la lotta alla criminalità informatica risale al 2008. La soluzione si basa su un'architettura IT obsoleta. È lenta, dispendiosa in termini di manutenzione e non riesce più a far fronte alle sfide sempre crescenti nella lotta agli abusi dei nomi a dominio.

Lotta agli abusi moderna e promettente

Nell'ambito del progetto «Domain Abuse 4.0» è in fase di sviluppo una nuova soluzione software all'avanguardia, basata su tecnologie moderne e sulla più recente infrastruttura «Switch Cloud». Il team di sviluppo del registry e il team di sviluppo del CERT uniscono le loro esperienze e competenze per sviluppare una soluzione rapida, a bassa manutenzione e altamente scalabile. Anche i processi vengono rielaborati e adeguati alle nuove circostanze, e i nostri esperti vengono formati al riguardo. Grazie a queste misure, Switch si conferma leader a livello mondiale nella lotta alla criminalità informatica.

Domain Abuse 4.0

Fatti e cifre

- 20 workflow (processi contro l'abuso) sono stati definiti sulla base dell'ODIn.
- 14 componenti software devono essere rinnovati o sviluppati.
- Sono state scritte più di 50 user story (non ancora definitive).
- Sono state valutate 16 varianti di soluzione.
- Finora hanno lavorato al progetto 12 persone in posizioni diverse.



Fondazione dell'European TLD ISAC

Sotto l'egida di CENTR, nel 2023 è stato fondato l'European TLD Information Sharing and Analysis Centre (ISAC).

Il Centro europeo per lo scambio di informazioni e l'analisi dei domini top level (European Top Level Domain Information Sharing and Analysis Center, TLD ISAC) mira a promuovere la sicurezza e la resilienza degli uffici di registrazione dei domini top level in Europa attraverso lo scambio di informazioni, la cooperazione e la condivisione di buone pratiche.

Riunisce operatori, esperti di sicurezza e altre parti interessate per scambiare informazioni sulle minacce, individuare nuove tendenze e sviluppare misure proattive per prevenire e contrastare gli attacchi informatici.

Switch, insieme ad altri operatori di ccTLD europei, è membro fondatore e partecipante attivo del comitato direttivo, del gruppo di lavoro e del gruppo «Threat Intelligence Sharing».

La prima conferenza TLD ISAC si è tenuta il 13 novembre 2023 a Bruxelles e Switch era rappresentata da due partecipanti.

Pagina web: <https://www.tld-isac.eu>



Web crawler

Nell'ambito della lotta alla criminalità informatica, verso la fine del 2023 Switch ha sviluppato un nuovo strumento: un web crawler che esamina sistematicamente le risorse pubblicamente accessibili nelle zone .ch e .li, al fine di individuare tempestivamente nomi a dominio compromessi o dannosi e scongiurare così il pericolo per gli utenti di Internet.

Per essere sempre aggiornati e poter lavorare in modo efficace, il nostro Cyber Threat Intelligence Team aggiorna regolarmente i criteri che ci aiutano a individuare i rischi. Ci confrontiamo attivamente anche con le autorità e con altri registry.

Se con il nostro crawler scopriamo nomi a dominio che commettono phishing o diffondono malware, dopo l'invio di una notifica al detentore e un periodo di attesa possiamo bloccare il nome a dominio.

Ciò significa che Switch può dare un importante contributo non solo in modo reattivo ma anche proattivo, attraverso la ricerca autonoma, per aumentare ulteriormente la sicurezza delle zone .ch e .li.

Nuova legge sulla protezione dei dati

Il 1° settembre 2023 è entrata in vigore la nuova legge svizzera sulla protezione dei dati. Switch ha avviato tempestivamente l'implementazione delle nuove disposizioni di legge.

Consulente per la protezione dei dati

Il 1° marzo 2023 Switch ha nominato un nuovo consulente per la protezione dei dati e ha informato l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT). Angelo Marchetta ricopre questa funzione per Switch e fornisce consulenza e supporto a Switch nell'applicazione delle norme sulla protezione dei dati e nella formazione dei collaboratori. Tra le sue mansioni rientrano anche il monitoraggio e il coordinamento di tutte le attività rilevanti di protezione dei dati all'interno dell'azienda. Inoltre, è incaricato della creazione di un sistema di gestione della protezione dei dati (DSMS).

Elenchi dei trattamenti

L'introduzione della disposizione relativa alla tenuta di un elenco dei trattamenti ha sostituito l'obbligo di notifica delle raccolte di dati precedentemente in vigore. Switch ha registrato le proprie attività di trattamento dei dati in qualità di gestore del registro da un lato nell'elenco interno dei trattamenti e dall'altro nel registro pubblico, il DataReg.

Sicurezza dei dati

Nell'ambito della nuova legge sulla protezione dei dati, Switch ha implementato alcune modifiche al processo di notifica delle violazioni della sicurezza dei dati. Ciò consente di segnalare rapidamente episodi che si prevede comportino un rischio elevato per la personalità o i diritti fondamentali della persona interessata.

DSMS

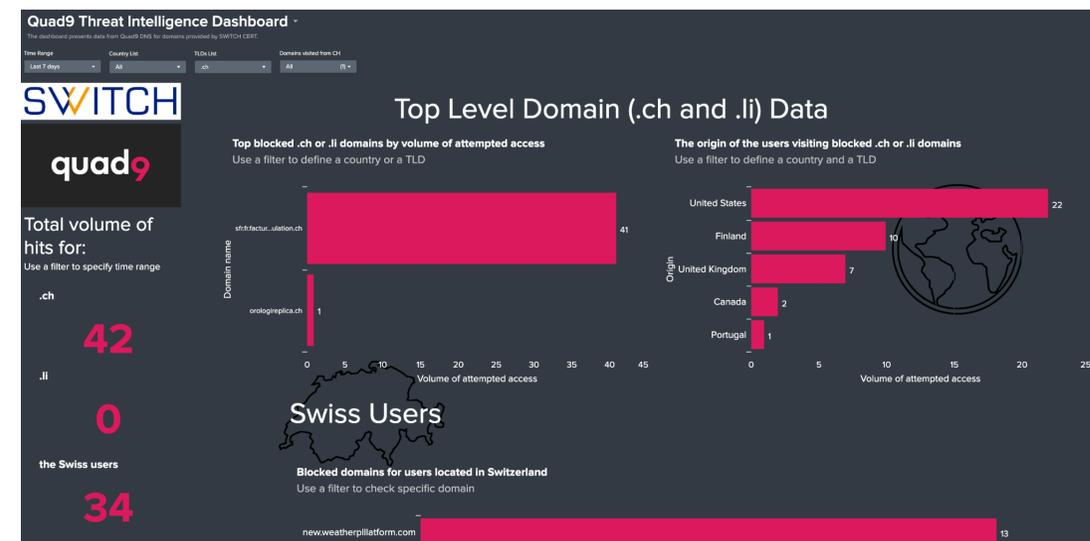
Switch attribuisce grande importanza alla protezione dei dati personali non solo dall'attuazione della nuova legge sulla protezione dei dati. In aggiunta al sistema di gestione della sicurezza dell'informazione ISMS, nei prossimi anni Switch svilupperà un sistema di gestione per la protezione dei dati, al fine di garantire sistematicamente la protezione dei dati e migliorarla costantemente.

Quad9: il ruolo della Threat Intelligence

Quad9 e Switch collaborano per analizzare le minacce all'Internet svizzero. Ciò comprende, tra le altre cose:

- Sviluppo e implementazione di una strategia di condivisione delle informazioni sulle minacce per Quad9 e per Domain Abuse presso Switch.
- Analizzare le principali minacce mensili bloccate da Quad9 in tutto il mondo e redigere rapporti periodici da distribuire sia alla comunità di sicurezza interessata che alle organizzazioni governative locali di sicurezza informatica. Esempi di rapporti: [Q9 Cyber Insights Report](#), [Malawi Report](#)
- Acquisire nuove partnership di informazioni sulle minacce per Quad9. Esempi: Phish Report, [SISA](#)
- Interventi su temi relativi ai dati sulle minacce, Quad9 e protezione dei dati. Conferenze: [Swiss Web Security Day](#), M3AAWG, [Women in Cyber](#)

- Creazione di un «Quad9 Threat Intelligence Product per Switch CERT». Lo scopo di questo progetto era quello di sviluppare una soluzione per Switch CERT per raccogliere, aggregare e analizzare i dati sulle minacce del Quad9 DNS. I risultati sono stati utilizzati per lo Switch Threat Radar e presentati in occasione del Swiss Web Security Day.



Principali minacce per il web svizzero

Sulla base dei dati raccolti da Quad9, nel 2023 erano in atto le seguenti campagne, che hanno rappresentato un pericolo per gli utenti Internet svizzeri:

Fake jQuery Domain

L'infezione viene iniettata in file Javascript legittimi ed esegue uno script dal dominio maligno jqueryns[.]com, che reindirizza a diversi siti fraudolenti. Sono stati colpiti soprattutto i siti web WordPress vulnerabili. Più di 8'000 richieste DNS sono state bloccate da Quad9 in Svizzera e 47 nomi a dominio .ch sono stati coinvolti.

WordPress SocGhosh injection

SocGhosh è una campagna malware diffusa e pluriennale che mira a distribuire aggiornamenti del browser falsi, anche agli utenti di Internet svizzeri. Una volta installati, gli aggiornamenti del browser falsi infettano il computer della vittima con diversi tipi di malware, tra cui trojan di accesso remoto (RAT). In un mese sono state bloccate da Quad9 circa 1'700 richieste DNS dalla Svizzera.

Phishing contro la Posta Svizzera

La pagina di phishing contro la Posta Svizzera era ospitata su campaign-image[.]eu. La campagna è stata attiva tra il 20 e il 26 aprile. In Svizzera, in aprile, più di 870 query sono state bloccate da Quad9 in una settimana. Più di 24'900 query sono state bloccate da Quad9 in tutto il mondo.

Malware «ndsw/ndsx»

Si tratta di un'altra variante del malware SocGhosh. Tutte le varianti del malware contengono l'istruzione «if(ndsw===undefined)», da cui il nome. L'obiettivo è installare il malware cosiddetto «Fake Update» sui computer Windows. 92 nomi a dominio .ch sono stati colpiti.

Black Hat Ad Network e Balada Injector

Si tratta di una campagna massiccia che utilizza i siti web WordPress hackerati come piattaforma di inventario per il posizionamento di annunci e reindirizzamenti. I siti web infetti reindirizzano a falsi aggiornamenti del browser e a truffe di finto supporto. 37 nomi a dominio .ch colpiti.

Nuova sede a Losanna

Il 2 maggio 2023, Switch ha aperto una sede nella Svizzera occidentale. Nell'EPFL Innovation Park, la fondazione ha assunto uffici per un massimo di 15 collaboratori. Tom Kleiber, amministratore delegato di Switch, spiega il fattore principale di questo passaggio con queste parole: «Per poter svolgere meglio e in modo più credibile il nostro ruolo nazionale nel settore universitario, abbiamo bisogno di una sede nella Svizzera occidentale. La vicinanza alla community e il confronto diretto con essa sono per noi molto importanti.»

Nel suo discorso in occasione dell'inaugurazione, Martin Vetterli, presidente dell'EPFL, si è espresso positivamente sulla nuova sede: «Le università della Svizzera romanda non vedono l'ora di rafforzare la collaborazione con Switch.»

Anche il registry è così più vicino ai registrar specializzati nella Svizzera romanda. Inoltre, la nuova sede nella Svizzera romanda offre ai talenti locali l'opportunità di impegnarsi nella regione per compiti significativi come l'utilizzo sostenibile dei dati della ricerca, la sicurezza informatica o le identità digitali.



Martin Vetterli, EPFL; Tom Kleiber, Switch; Claudia Lienert, Switch; Alexandre Gachet, Consiglio di fondazione Switch

IPv6 Evangelist

Switch si impegna dal 1996 per l'introduzione dello standard IPv6, che consideriamo essenziale per lo sviluppo sostenibile di Internet. Oltre all'implementazione nella rete universitaria e presso il registry abbiamo anche sostenuto le relative attività della community Internet svizzera, sotto forma di eventi quali conferenze e corsi, lavori di standardizzazione nell'ambito dell'Internet Engineering Task Force (IETF) e consulenza agli organi politici.

In questo modo abbiamo contribuito a far sì che la Svizzera sia da molti anni uno dei paesi in cui IPv6 è ben consolidato e continua a diffondersi.

Questi sforzi sono stati riconosciuti nel 2023 dal forum internazionale IPv6 quando Simon Leinen, collaboratore di lunga data di Switch, è stato accolto nella [IPv6 Hall of Fame](#) come «IPv6 Evangelist». Attualmente nel mondo ci sono solo circa 100 «IPv6 Evangelists».



Sondaggio clientela registrar

A novembre/dicembre 2023, Switch ha condotto un sondaggio sulla soddisfazione dei clienti presso tutti i registrar, ottenendo la partecipazione di 30 soggetti su 156. I risultati hanno pertanto carattere indicativo.

L'essenziale in breve

- Per i registrar Switch è sinonimo di massima affidabilità, sicurezza, stabilità, simpatia, attenzione alla qualità e competenza.
- I partecipanti al sondaggio ritengono che Switch, rispetto a tutti i grandi registry mondiali, offra un servizio complessivo di gran lunga superiore.
- L'immagine generale che i registrar hanno di Switch raggiunge un livello molto elevato, con 8.7 punti su un massimo di 10.

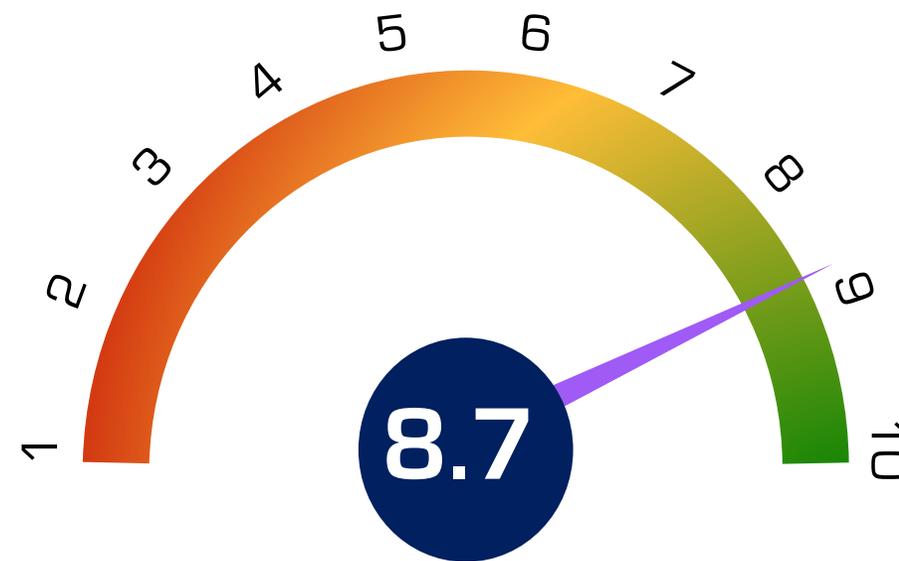


Immagine generale di Switch

Domanda: Considerando tutte le vostre informazioni su Switch come registry, qual è la vostra immagine generale di Switch?

Scala: 1 = estremamente negativo; 10 = estremamente positivo

3.

Rapporto d'attività – Statistiche

50%

Il programma di resilienza DNS ha dato alle DNSSEC la svolta auspicata. Nel frattempo, quasi il 50% dei nomi a dominio è stato autenticato.

1.6%

Crescita del dominio .ch

40'000

Incremento di circa 40'000 nomi a dominio.

Portafoglio nomi a dominio .ch – Evoluzione nel 2023

Evoluzione .ch

In un anno il numero di nomi a dominio .ch è aumentato di ben 40'000 unità. Si tratta di un aumento dell'1.6% rispetto all'anno precedente.

| | 2022 | 2023 |
|--|------------------|------------------|
| Nuove registrazioni | 281'610 | 294'195 |
| Cancellazioni | 258'724 | 282'649 |
| Riattivazioni* | 31'097 | 29'958 |
| Numero di domini al 31 dicembre | 2'521'444 | 2'562'914 |

Evoluzione .li

In un anno il numero di nomi a dominio .li è rimasto pressoché invariato.

| | 2022 | 2023 |
|--|---------------|---------------|
| Nuove registrazioni | 10'094 | 10'658 |
| Cancellazioni | 10'178 | 12'218 |
| Riattivazioni* | 1'823 | 1'699 |
| Numero di domini al 31 dicembre | 70'478 | 70'607 |

Evoluzione del portafoglio di nomi a dominio .ch e .li

* Nomi a dominio cancellati e riattivati dal registrar entro 40 giorni.

Servizio informazioni – Statistiche 2023

Servizio informazioni

A ogni persona che fornisce prova attendibile del proprio legittimo interesse prioritario, Switch concede accesso gratuito ai dati personali contenuti nel database RDDS (Whois) del detentore del nome a dominio in questione. Questa statistica comprende tutte le richieste pervenute nell'anno in esame attraverso i moduli del Servizio informazioni. Il numero di richieste è rimasto molto vicino all'anno precedente.

| | Privato | Autorità |
|--------------------------|------------|------------|
| Informazioni fornite | 304 | 135 |
| Informazioni non fornite | 56 | 5 |
| Richieste generali * | 4 | 0 |
| Totale richieste | 364 | 140 |

* In questi casi si tratta di richieste riguardanti processi, procedure e basi legali.

Accesso semplificato tramite RDAP per .ch e .li

Se un'autorità o un'organizzazione possiede le necessarie autorizzazioni, può richiedere i nomi a dominio con dati personali tramite RDAP (Registration Data Access Protocol). Nel 2023 il numero delle autorità è aumentato notevolmente, anche a causa della nostra migliore interconnessione con le autorità di perseguimento penale. Alla fine del 2022 solo 5 autorità utilizzavano l'RDAP, mentre alla fine del 2023 erano già 18. La quota maggiore è rappresentata dalle polizie cantonali.

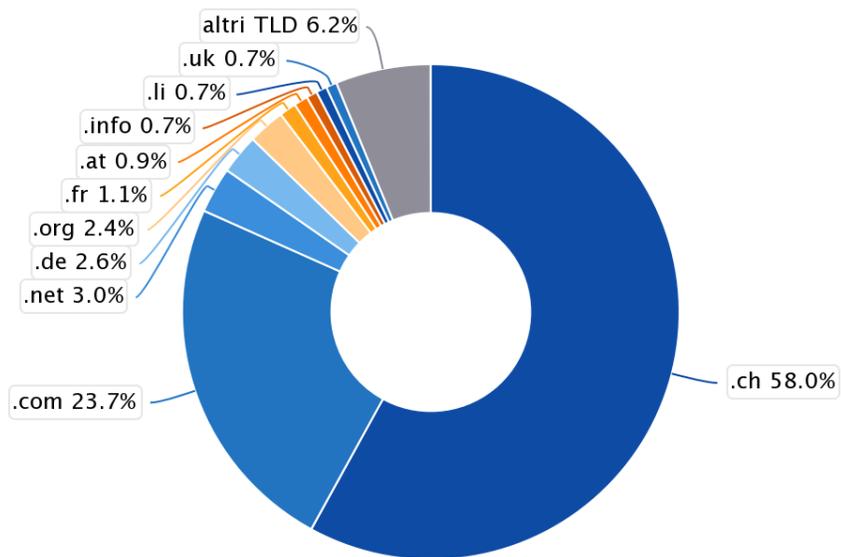
| | Richieste |
|--------------------------|--------------|
| Informazioni fornite | 3'612 |
| Informazioni non fornite | 309 |
| Totale richieste | 3'921 |

Quota di mercato di .ch e .li presso detentrici e detentori svizzeri di nomi a dominio

La quota di mercato dei TLD (domini top level) .ch presso detentrici e detentori in Svizzera non ha pressoché subito variazioni da ottobre 2022 a ottobre 2023.

Ottobre 2022

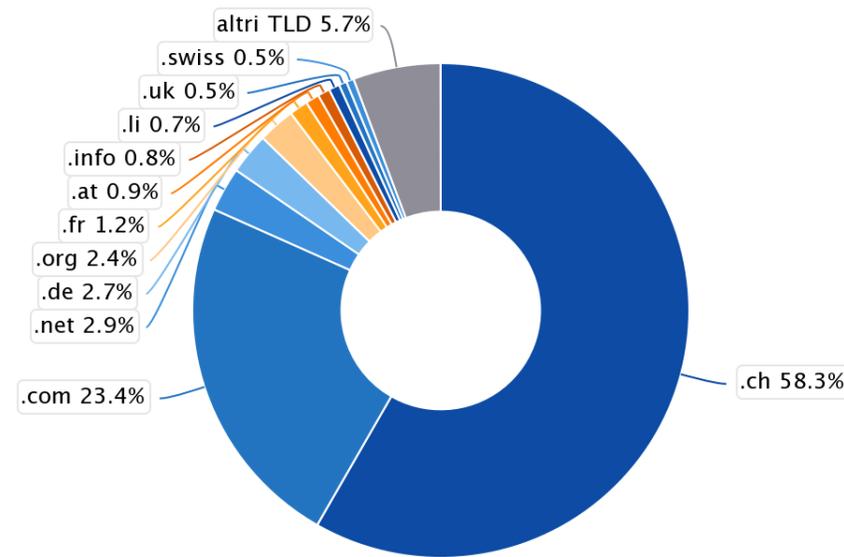
Quota di mercato dei vari TLD presso detentrici e detentrici di nomi a dominio in Svizzera. Fonte: CENTR



Nella quota di mercato dei TLD generici .com/.net/.org le variazioni sono state minime, così come per il TLD .li.

Ottobre 2023

Quota di mercato dei vari TLD presso detentori e detentrici di nomi a dominio in Svizzera. Fonte: CENTR



Programma di resilienza DNS – Evoluzione in cifre

DNSSEC

- Percentuale di nomi a dominio .ch con DNSSEC, aggiornamento al 1° gennaio 2024: 49.1% (1° gennaio 2023: 44.8%).
- Percentuale di errori: nel corso dell'anno il tasso di errore è rimasto più o meno costante a un livello molto basso. Meno dello 0.25% di tutti i nomi a dominio DNSSEC presentava errori (2022: meno dello 0.5%).

DMARC e SPF

- 1° luglio 2023 (inizio delle misurazioni con OpenIntel): 2.6% configurati correttamente.
- 1° gennaio 2024 4.5% configurati correttamente. Cifre per nomi a dominio .ch e .li, configurazione corretta sia di DMARC che di SPF. Dati secondo le statistiche del fornitore di servizi di misurazione esterno.

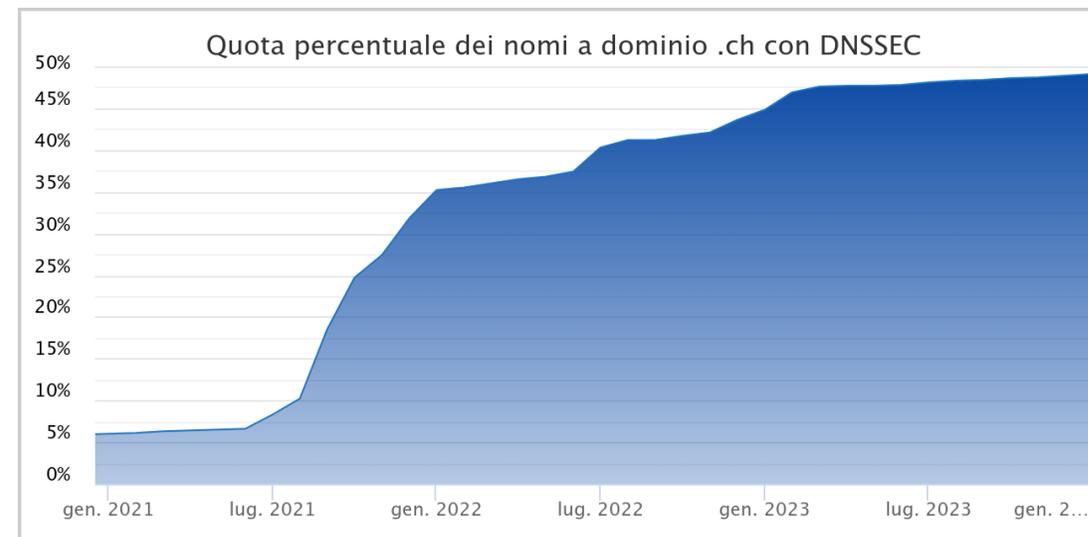
[Statistiche DNSSEC di Switch](#)

[Statistiche di OpenIntel](#)

Calcolo del rimborso per l'anno 2023

- Entrate supplementari raccolte dalla differenziazione dei prezzi: CHF 1'792'697
- Al netto della compensazione fissa per Switch e il fornitore di servizi di misurazione esterno 2023: CHF – 444'907
- Totale rimborso CHF 1'347'790

I rimborsi saranno effettuati a fine febbraio 2024.



Evoluzione di DNSSEC

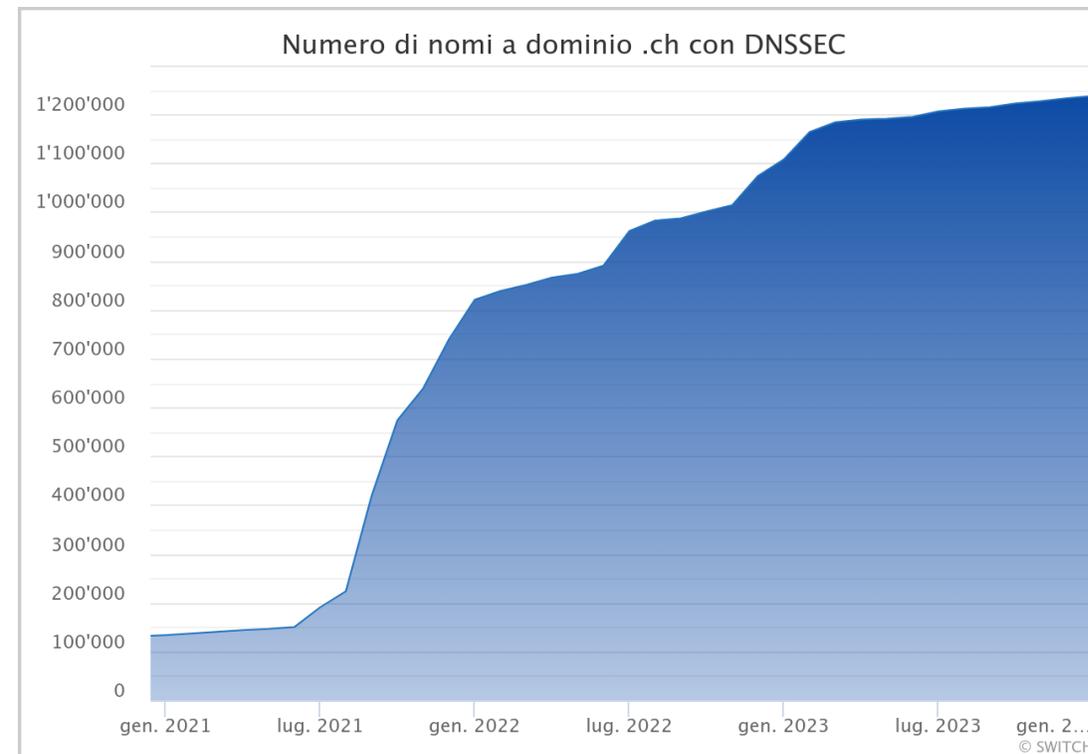
Numero di nomi a dominio autenticati

Alla fine del 2023, oltre 1.2 milioni di nomi a dominio .ch sono autenticati con DNSSEC.

Si tratta di una quota di quasi il 50% di tutti i nomi a dominio .ch con name server, rispetto al 45% alla fine del 2022 e al 35% alla fine del 2021. Il forte aumento registrato nel 2021 e nel 2022 è stato trainato principalmente dai registrar che, nell'ambito del programma di resilienza DNS, hanno autenticato tutti i nomi a i dominio dei propri clienti. Nel 2023 questa crescita ha subito un rallentamento.

Nel frattempo, i maggiori registrar svizzeri hanno autenticato i loro nomi a dominio per quanto possibile. Se i nomi a dominio hanno name server «esterni», i registrar non hanno alcuna influenza sull'autenticazione. Per i grandi registrar all'estero, il TLD .ch rappresenta solo una piccola parte del loro business, dunque l'onere dell'autenticazione non risulta molto conveniente. Di conseguenza, in futuro la crescita dovrebbe subire un forte rallentamento.

Numero di nomi a dominio .ch con DNSSEC



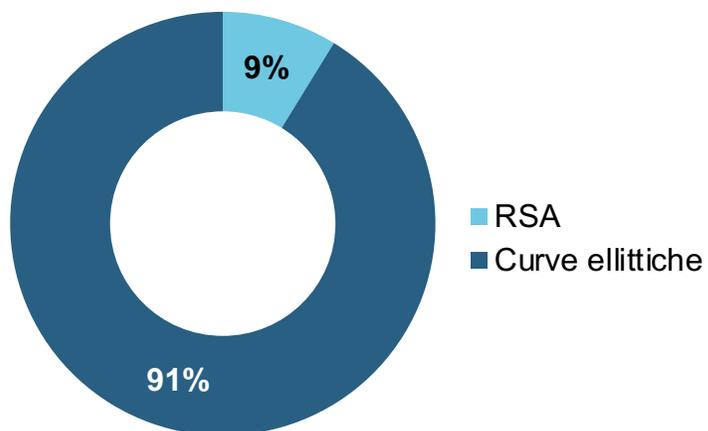
1'237'670 nomi a dominio .ch autenticati con DNSSEC il 1° gennaio 2024

Evoluzione di DNSSEC

Distribuzione di algoritmi DS

Attualmente, oltre il 90% di tutti i nomi a dominio .ch utilizza l'algoritmo 13 attualmente consigliato (ECDSAP256SHA256).

I record DS con algoritmi 5 e 7, che non sono più considerati sicuri a causa della loro autenticazione SHA-1, non sono più supportati da febbraio 2023 e sono stati pertanto rimossi dalla zona.



Autorizzazioni DNSSEC utilizzate

| Algoritmo DNSSEC | Numero | Percentuale |
|------------------------|-----------|-------------|
| 5 – RSASHA1 | 0 | 0.00% |
| 7 – RSASHA1-NSEC3-SHA1 | 0 | 0.00% |
| 8 – RSASHA256 | 111'923 | 9.04% |
| 10 – RSASHA512 | 59 | 0.00% |
| 13 – ECDSAP256SHA256 | 1'225'464 | 90.93% |
| 14 – ECDSAP384SHA384 | 142 | 0.01% |
| 15 – ED25519 | 42 | 0.00% |
| 16 – ED448 | 90 | 0.00% |

Validazione DNSSEC in Svizzera

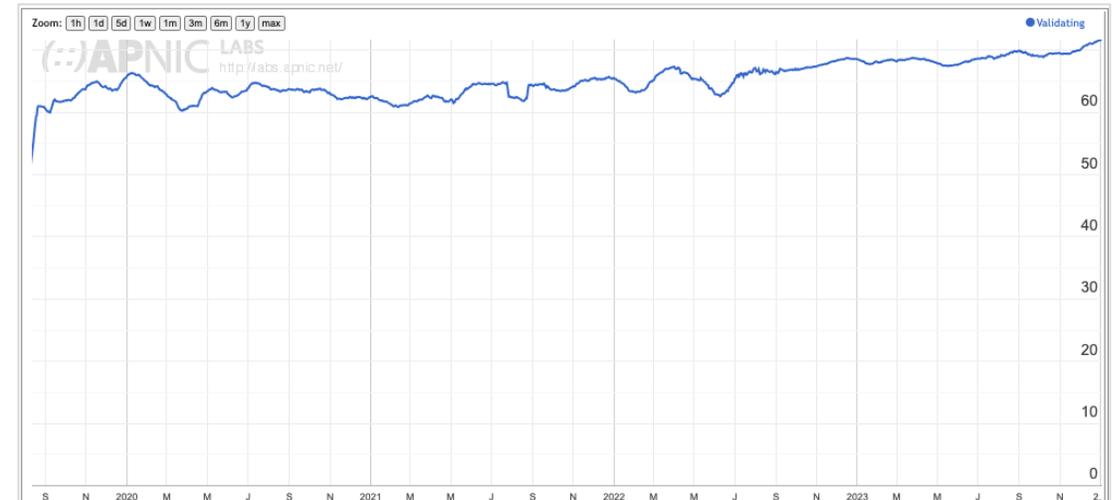
Validazione DNSSEC

Affinché gli utenti siano protetti dal DNS spoofing, i nomi a dominio devono essere autenticati, ma queste autenticazioni devono essere convalidate dal resolver DNS.

In base alle misurazioni di APNIC, il tasso validazione DNSSEC sui resolver degli ISP svizzeri lo scorso anno è salito per la prima volta oltre il 70%.

Sito web: <https://stats.labs.apnic.net/dnssec/CH>

Validazione DNSSEC su resolver svizzeri



Deferred Delegation – Status

Basi legali

Con l'art. 25 dell'ODIn «Condizioni generali di attribuzione», l'UFCOM ha posto le basi legali che consentono al registry di non attivare un nome a dominio se vi è il sospetto che questo possa essere utilizzato a scopo illecito o in modo illecito e di non registrare i name server nel zone file. Tale processo è noto con il nome di «Deferred Delegation».

Adeguamenti del processo

Attraverso l'inasprimento delle regole, nel 2023 siamo riusciti a trattenere e a cancellare un numero significativamente maggiore di registrazioni.

Dopo il passaggio alla fase produttiva, continuiamo a rivedere regolarmente i criteri. Sono inoltre allo studio nuovi criteri e metodi di verifica per individuare meglio le registrazioni abusive tenendo sempre in considerazione gli utenti autorizzati, che non devono essere ostacolati.

Siamo in contatto con altri registry per migliorare ulteriormente e scambiare esperienze.

Abbiamo sviluppato una dashboard che ci consente di avere sempre una panoramica delle metriche attuali del processo. I criteri vengono periodicamente rielaborati e perfezionati attraverso l'analisi dei dati. La Deferred Delegation dovrebbe mirare il più possibile solo all'utilizzo improprio, senza ostacolare gli utenti autorizzati.

Dati Deferred Delegation 2023

| | |
|----------------------------|---------|
| Totale nuove registrazioni | 294'195 |
| Nomi a dominio deferred | 2'751 |
| Nomi a dominio cancellati | 1'956 |

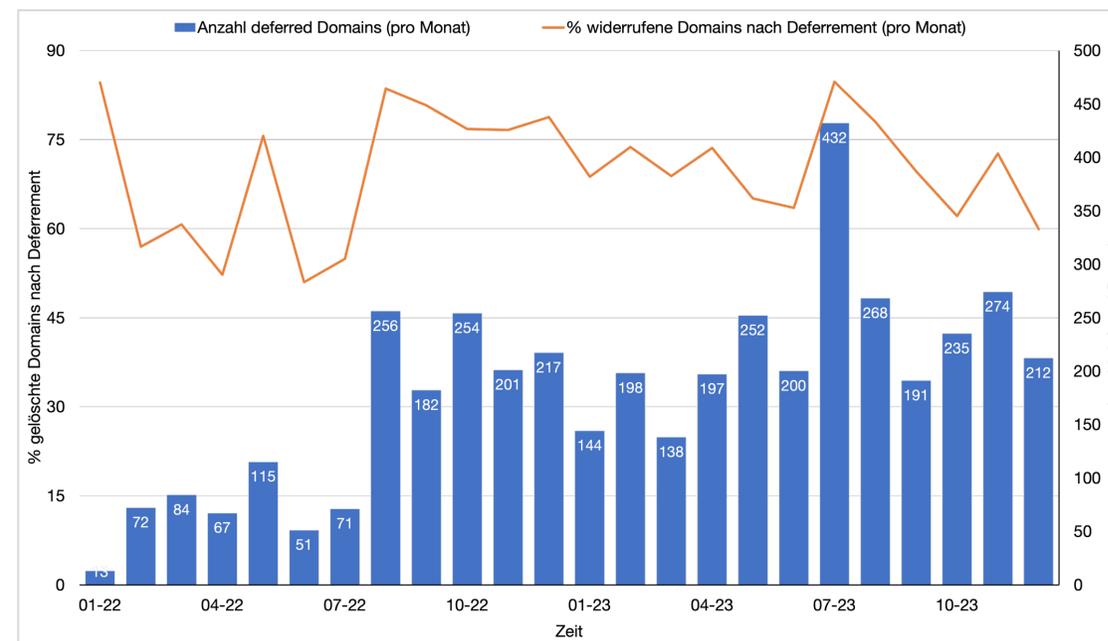
Deferred Delegation – Status

Una retrospettiva della Deferred Delegation

Dall'introduzione della deferred Delegation all'inizio del 2022, abbiamo lentamente aumentato il numero di nomi a dominio «deferred» (barre blu).

Questo risultato è stato raggiunto grazie a criteri sempre più severi. Con un'attenta selezione di tali criteri è stato possibile mantenere stabile la percentuale di nomi a dominio che venivano revocati dopo la mancata identificazione del detentore (curva arancione).

Salta all'occhio l'elevato numero di nomi a dominio «deferred» a luglio 2023. Una parte è da ricondurre a un detentore che aveva registrato un gran numero di nomi a dominio senza però fornire alcuna identificazione in un secondo momento.



Composizione delle controversie

Switch ha ricevuto dall'UFCOM l'incarico di offrire un servizio gratuito di composizione delle controversie. A tal fine, dal 2004 Switch si avvale del servizio di composizione delle controversie di WIPO (World Intellectual Property Organization). WIPO gestisce un servizio di composizione delle controversie accreditato da ICANN per oltre 70 registry.

Nel 2023, gli esperti si sono espressi in merito a 16 nomi a dominio .ch. La decisione degli esperti è l'ultima fase del processo. Un numero leggermente inferiore di casi viene chiuso prima, ad esempio durante l'arbitrato o a causa dell'interruzione del procedimento.

| Decisione WIPO | 2022 | 2023 |
|--------------------------|-----------|-----------|
| Trasmessa ai richiedenti | 15 | 11 |
| Accuse respinte | 2 | 5 |
| Numero decisioni | 17 | 16 |

Decisioni di WIPO (situazione a febbraio 2024)

| | Nomi a dominio |
|--------------------------|---|
| Trasmessi ai richiedenti | diadora.ch immoswisslife.ch albi-keramik.ch albikeramik.ch migrosbankswitzerland.ch naturoflooring.ch dallmayer.ch tmhinternational.ch solidea.ch nortonabrasives.ch dermagora.ch |
| Accuse respinte | rockantenne.ch cheeze.ch schluessel-luzern.ch imageskincare.ch zoskinhealth.ch |

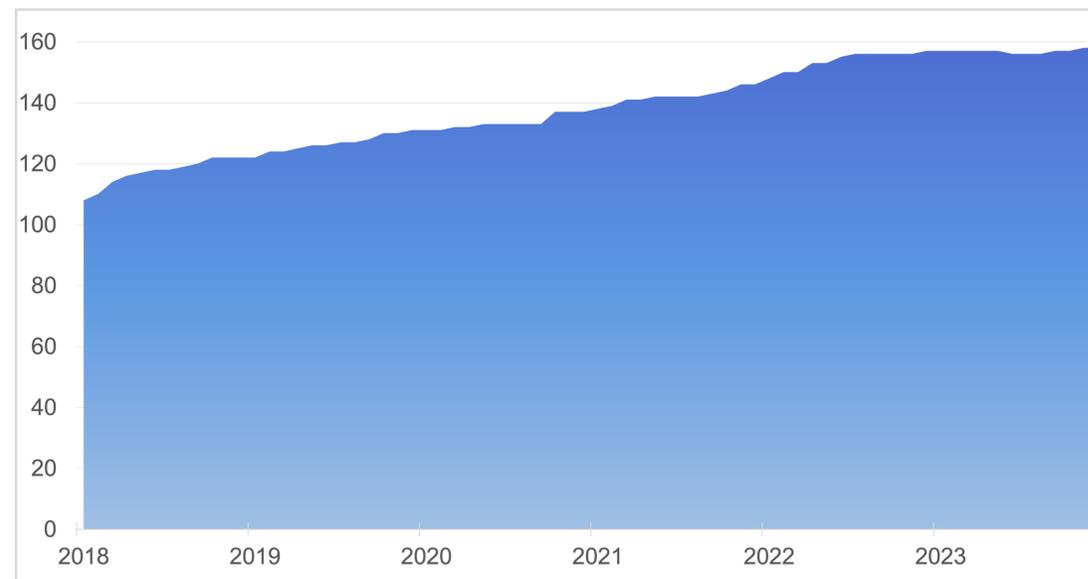
Evoluzione dei registrar

Il 2018 ha visto l'arrivo di un numero di registrar superiore alle aspettative, per un totale di 122 a fine anno.

Nel 2019 il numero di registrar è salito a 131 e a fine 2020 il settore registry contava 137 registrar. Nel 2021 il numero dei registrar è aumentato di 9, per un totale di 146.

Nel 2022, 11 registrar hanno sottoscritto per la prima volta un contratto di prova per l'accesso al sistema di test. Terminata con successo la fase pilota e superata la prova, siamo riusciti ad attivare questi registrar in maniera produttiva. Il numero totale dei registrar riconosciuti è arrivato così a 157.

Nel 2023 siamo riusciti a consentire l'accesso al sistema produttivo solo a un altro registrar e il numero è salito a 158.



Performance dei name server

Per i requisiti di misurazione della performance del DNS relativamente ai tempi di risposta a richieste del DNS, Switch si rifà all'accordo ICANN: le richieste alla zona CH devono ricevere risposta da almeno un name server logico entro 500 ms (UDP) o 1500 ms (TCP).

Requisito sempre soddisfatto nel 2023.

Le misurazioni sono effettuate da RIPE e sono consultabili dal pubblico.

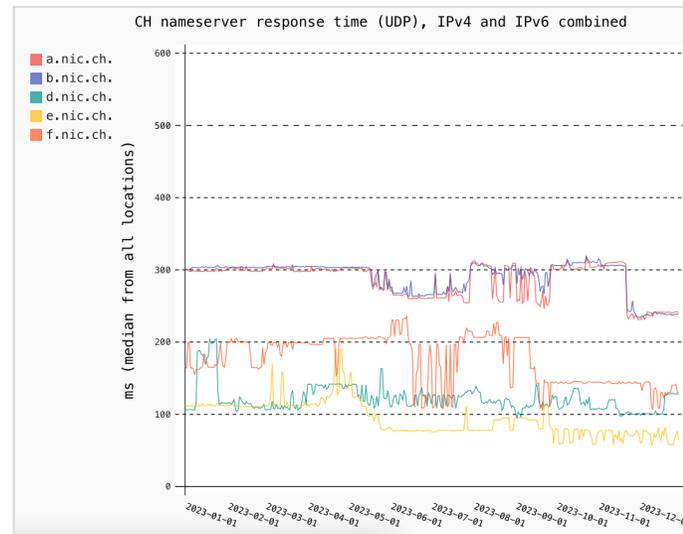
<https://atlas.ripe.net/dnsmon/group/ch>

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

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

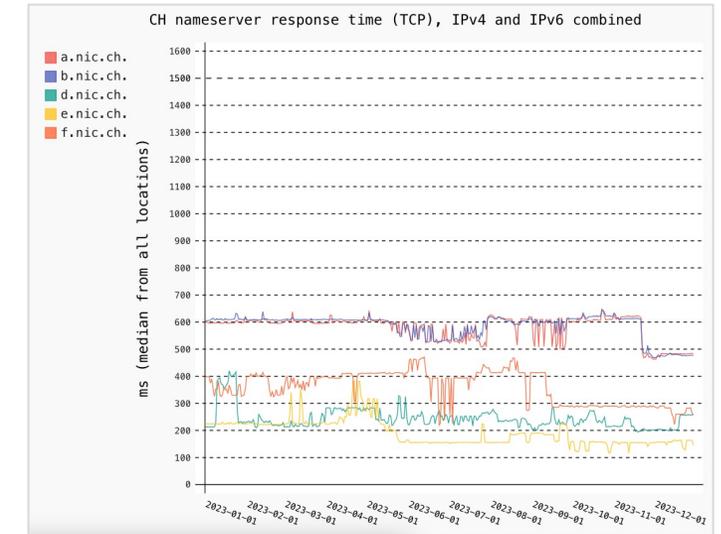
Tempi di risposta UDP

Tempi di risposta combinati di IPv4 e IPv6



Tempi di risposta TCP

Tempi di risposta combinati di IPv4 e IPv6



Criminalità informatica

Dati quantitativi

Nell'anno in esame sono stati acquisiti e trattati i seguenti casi:

Numero di casi di malware e phishing 2023

Osservazione quantitativa

| | # malware | # phishing |
|--|--------------|------------|
| Segnalazioni pervenute | 1'242 | 942 |
| Sospetti confermati | 505 | 643 |
| Numero di nomi a dominio bloccati | 187 | 475 |
| Motivazione per la sospensione del blocco: | | |
| - Durata legale superata | 37 | 17 |
| - Eliminati dopo il blocco | 119 | 34 |
| - Ancora in elaborazione | 4 | 12 |
| Nomi a dominio revocati | 27 | 419 |

Dati qualitativi

I casi sono stati trattati con queste tempistiche:

Numero di casi di malware e phishing 2023

Osservazione qualitativa

| | Durata | |
|---|----------------|-----------------|
| Durata del blocco secondo l'art. 15 dell'ODIn, cpv. 1, 2, 3 max. tempo di blocco 30 giorni (720 h) | Durata minima | 0.50 h |
| | Media | 103.32 h |
| | Durata massima | 160.05 h |
| Tempi reazione di Switch dopo segnalazione | Media | 8.15 h |
| Tempo di eliminazione della minaccia dopo la comunicazione al detentore | Media | 104.27 h |

DNS Health Report

Il DNS Health Report verifica la raggiungibilità dei name server e nomi a dominio .ch e .li. In caso di problemi tecnici, Switch informa i gestori e fornisce raccomandazioni su come eliminare i malfunzionamenti. In questo modo, il DNS Health Report garantisce l'affidabilità della connessione Internet in Svizzera. Oggetto della verifica:

- Name server: si verifica se la funzione dei name server corrisponde agli standard DNS.
- Nomi a dominio: si verifica se i nomi a dominio autenticati con DNSSEC possono essere risolti tramite un resolver ricorsivo per la convalida.

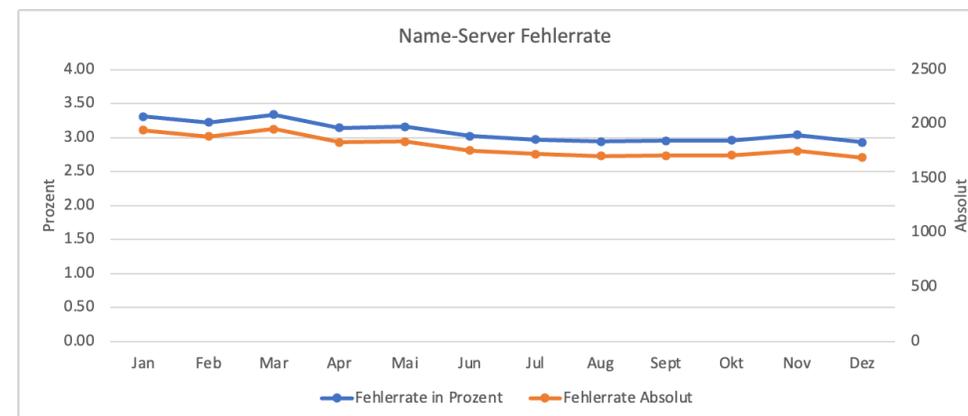
Report sui name server

Il margine di errore nella misurazione di raggiungibilità dei name server diminuisce solo leggermente ma con costanza dall'inizio delle misurazioni. Una tendenza molto soddisfacente.

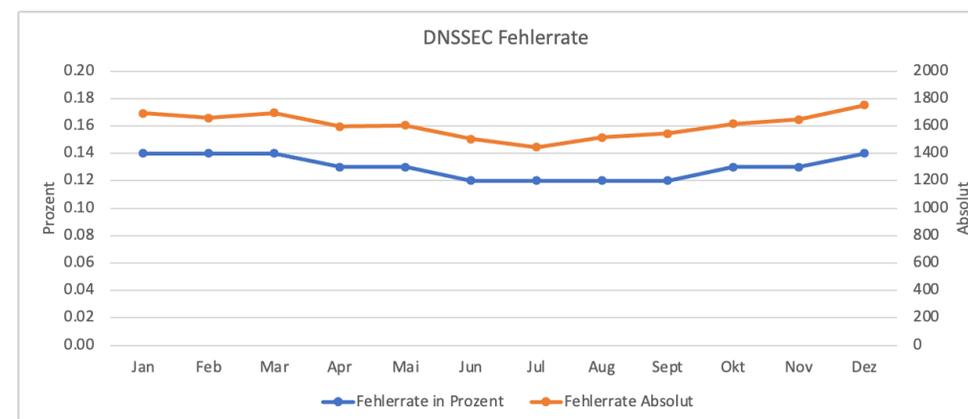
Report sui nomi a dominio

Il margine di errore nella misurazione di raggiungibilità dei nomi a dominio ha raggiunto un plateau. La maggior parte dei nomi a dominio che presentano errori sono nomi a dominio temporanei per i quali la motivazione a correggere gli errori è scarsa.

Margine di errore nella misurazione di raggiungibilità dei name server



Margine di errore nella misurazione di raggiungibilità dei nomi a dominio



DAAR .ch

ICANN Domain Abuse Activity Reporting

Con la pubblicazione della zona .ch, Switch aderisce al progetto DAAR (Domain Abuse Activity Reporting) di ICANN. Il progetto mette a confronto le segnalazioni dei casi di sospetto abuso per i diversi TLD.

Il programma così come i report per ccTLD sono ancora allo stato Beta. Il grafico, tuttavia, consente di fare già un primo confronto tra .ch e gli altri ccTLD e gTLD.

Cosa si misura?

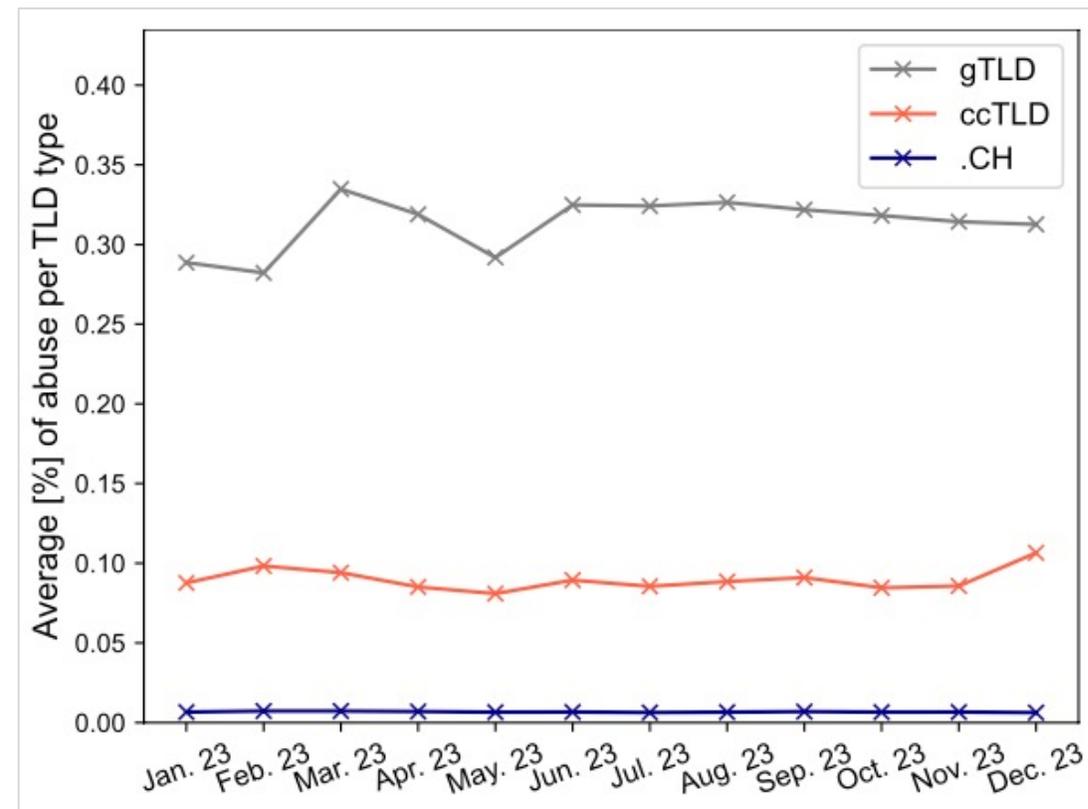
Percentuale dei nomi a dominio .ch che sono stati identificati come una minaccia per la sicurezza a confronto con il numero medio dei nomi a dominio in altre zone TLD.

Per informazioni dettagliate consultare il sito di ICANN:

<https://www.icann.org/octo-ssr/daar>

Analisi di .ch

Il report DAAR mostra come l'abuso dei nomi a dominio presso ccTLD .ch sia basso rispetto alla media di tutti i TLD. Si tratta quindi di una conferma dell'efficacia delle misure messe continuamente in campo per contrastare i crimini informatici così come della bontà della collaborazione con le autorità svizzere e le organizzazioni internazionali.



DAAR .li

ICANN Domain Abuse Activity Reporting

Con la pubblicazione della zona .li, Switch aderisce al progetto DAAR (Domain Abuse Activity Reporting) di ICANN. Il progetto mette a confronto le segnalazioni dei casi di sospetto abuso per i diversi TLD.

Il programma così come i report per ccTLD sono ancora allo stato Beta. Il grafico, tuttavia, consente di fare già un primo confronto tra .li e gli altri ccTLD e gTLD.

Cosa si misura?

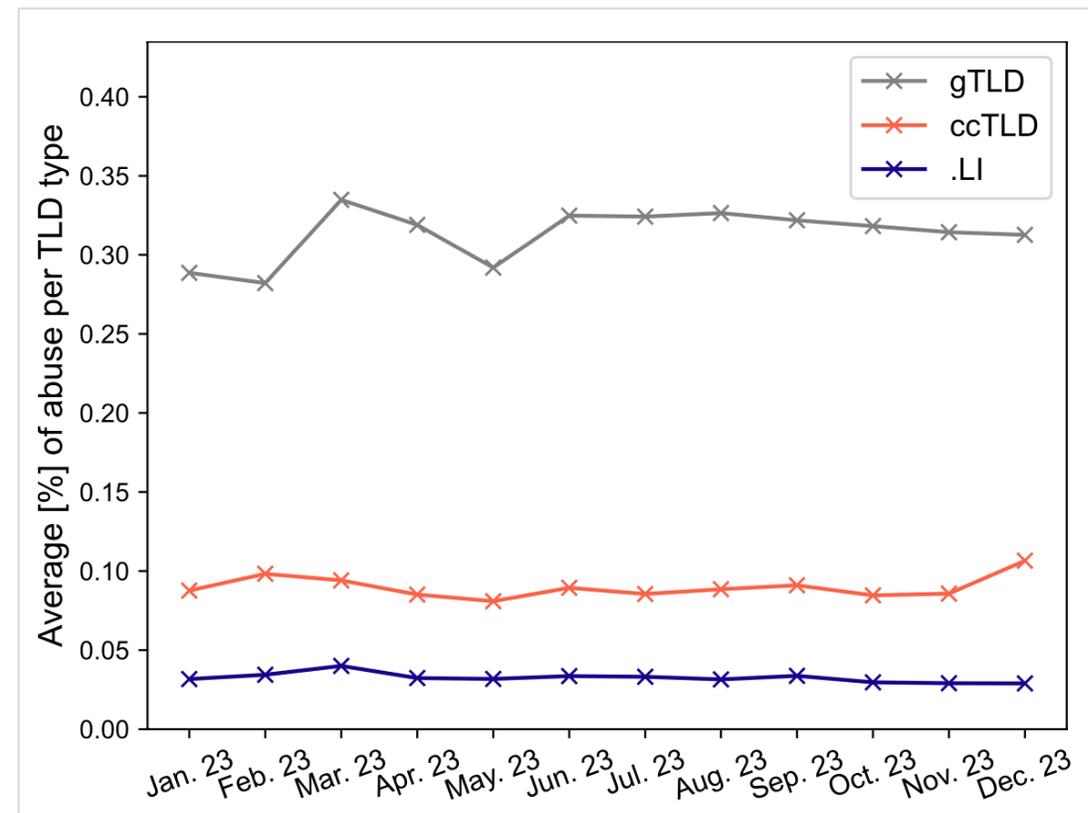
Percentuale dei nomi a dominio .li che sono stati identificati come una minaccia per la sicurezza a confronto con il numero medio dei nomi a dominio in altre zone TLD.

Per informazioni dettagliate consultare il sito di ICANN:

<https://www.icann.org/octo-ssr/daar>

Analisi di .li

Il report DAAR mostra come sia stato possibile eliminare l'abuso dei nomi a dominio nel ccTLD .li, ad eccezione di poco meno di due dozzine di nomi a dominio. Sarà possibile mantenere basso questo valore solo se la collaborazione tra il registry e le autorità continuerà ad essere così proficua.



4.

Rapporto d'attività – Dati economici

Dati economici

Alla riunione del Consiglio di fondazione del 13 giugno 2024 sarà approvato il Rapporto annuale 2023 della Fondazione Switch, insieme a stato patrimoniale e conto economico. La pubblicazione è prevista per il 14 giugno 2024.

Non si pubblicano dati in questa sede, rimandando alla documentazione completa del Rapporto annuale 2023 di Switch.

5.

Rapporto d'attività – Sviluppi

Uno sguardo al 2023

Cambio dell'algoritmo DNSSEC

Per l'autenticazione del zone file è stato inizialmente scelto l'algoritmo NSEC3 (con opt-out). Questo meccanismo impediva il cosiddetto «zone walking», rendendo più difficile l'elencazione automatica di tutti i nomi a dominio con la tipica conseguenza delle ondate di spam.

Nel frattempo, il zone file è pubblico. Il tasso di autenticazione elevato al 50% richiede metodi più efficienti. Ciò è possibile con il passaggio all'algoritmo NSEC. La modifica dei parametri di sicurezza nel DNS richiede accurati accertamenti tecnici preliminari. Sono coinvolti i gestori dei name server e dei resolver. È stata consultata anche la community tecnica di ICANN e DNS-OARC. È stato così possibile dare il via libera al passaggio, che si è svolto il 10 novembre 2023 e non ha comportato alcuna compromissione delle funzioni dei name server o dei resolver. Dopo il cambio, il zone file è leggermente più grande, mentre i name server e i resolver necessitano di meno risorse di calcolo.

European TLD ISAC

A febbraio 2023 è stato fondato l'European TLD ISAC (Information Sharing and Analysis Center). La fase costitutiva è supportata da CENTR e da sette registry ccTLD. Switch è rappresentata nel Board e fornisce un collaboratore per l'elaborazione dei processi di collaborazione. L'attenzione deve essere rivolta allo scambio di informazioni sulle minacce, motivo per cui qui sono attivi soprattutto i registry con un CERT e un ISMS. È previsto un periodo di due anni per lo sviluppo dei processi chiave e l'estensione a tutti i registry ccTLD dell'UE. L'European TLD ISAC è interamente finanziato dai registry partecipanti.

Uno sguardo al 2023

Aumento della sicurezza delle e-mail

Nel programma di resilienza DNS, in collaborazione con l'UFCOM e i registrar, è stato stabilito che nel 2024 l'implementazione di DMARC e SPF varrà come criterio per i rimborsi. In questo contesto, nel 2023 Switch ha creato l'infrastruttura di misurazione e una dashboard per la verifica manuale dei criteri di misurazione.

Per il 2025 è stato definito DANE come criterio. Su questo argomento, Switch ha offerto corsi di formazione a Losanna e Zurigo a ottobre 2023.

Di conseguenza, anche l'infrastruttura di posta elettronica interna di Switch è stata modificata in modo tale che tutti e tre i protocolli di sicurezza possano essere utilizzati per l'invio e per la verifica alla ricezione.

RDAP front-end web per autorità

Il front-end web per la banca dati RDDS (Whois) è in funzione. Ogni utente presso un'autorità firma un contratto per l'utilizzo. Switch si occupa della gestione dei diritti di utilizzo. Finora solo poche autorità di piccole dimensioni utilizzano questo comodo accesso, ma il front-end web è pensato proprio per queste autorità.

Prospettive strategiche e obiettivi

I singoli progetti pianificati sono presentati alla voce «Novità pianificate 2024». In un'altra sezione è presentato anche il progetto Domain Abuse 4.0, che sarà il focus principale del 2024. Qui, si tratta di due orientamenti di natura piuttosto strategica.

Ubicazione dell'infrastruttura

Negli ultimi cinque-otto anni, le grandi organizzazioni con le loro infrastrutture IT sono passate agli hyperscaler nel cloud, per consolidare l'infrastruttura e risparmiare sui costi. Le PMI hanno seguito questa tendenza un po' più tardi, anche sotto la pressione di fornitori di software come Microsoft, che non garantiscono più a lungo termine il funzionamento on-premise dei loro software.

L'infrastruttura IT di Switch è distribuita su diverse sedi, che sono collegate da un'infrastruttura in fibra ottica gestita autonomamente. Ciò garantisce il massimo controllo su tutti i livelli dei componenti IT.

La collaborazione con un fornitore di servizi cloud svizzero offre a Switch la possibilità di costruire nuovi componenti per computer e storage in centri di calcolo professionali. Qui è presente un livello più elevato di sicurezza contro i guasti e di controllo dell'accesso rispetto alle sedi finora offerte dalle università. Anche questi centri di calcolo sono allacciati alla rete in fibra ottica «Switch LAN».

Nel corso del 2024 e del 2025, i componenti software del registry passeranno a una nuova architettura e saranno operativi nelle nuove sedi. La governance dell'infrastruttura e dei dati archiviati è interamente di Switch e la sede dell'infrastruttura rimane in Svizzera. Si tratta di condizioni quadro importanti per la gestione di un'infrastruttura critica e per il trattamento dei dati nell'ambito della lotta alla criminalità informatica.

Prospettive strategiche e obiettivi

Programma di resilienza DNS 2027+

Il programma di resilienza DNS fa parte del contratto di rinnovo 2022 fino al 2026 con l'UFCOM. Il DNSSEC Advisory Board stabilisce quali protocolli di sicurezza debbano essere promossi dal programma di resilienza. I criteri vengono stabiliti sempre con due anni di anticipo. In questo modo Switch può offrire corsi di formazione e preparare l'infrastruttura di misurazione. I registrar hanno tempo a sufficienza per pianificare gli interventi tecnici per eventuali modifiche prima dell'inizio delle misurazioni.

L'eventuale proseguimento del programma dopo il 2026 e le relative modalità dovrebbero essere discusse nel 2024. Il programma in corso fornisce già importanti indicazioni ed esperienze. Per questa discussione si consiglia di riunire tutte le parti coinvolte.

Novità pianificate 2024

Programma di resilienza DNS: misurazioni DANE

Come criterio per i rimborsi nel 2025 è stato stabilito il protocollo di sicurezza DANE. Switch sta ampliando l'infrastruttura di misurazione di conseguenza. Anche la dashboard verrà ampliata, in modo che registrar e hosting provider possano verificare se la configurazione è stata implementata correttamente seguendo i consigli di Switch.

Il criterio per il 2026 sarà IPv6. A tal fine non sono previste formazioni specifiche.

Domain Abuse 4.0

Il progetto «Domain Abuse 4.0» assicura al registry il futuro della lotta alla criminalità informatica. Una descrizione del progetto è riportata a pagina 23.

ISMS ISO27001:2022

Finora la norma in base alla quale veniva effettuato l'audit del registry era la norma ISO 27001:2013. La norma rielaborata nella versione del 2022 tiene conto di un ambito tematico più ampio e adeguato alle esigenze tecnologiche e sociali.

Entro l'autunno del 2024 Switch prevede di adeguare tutti i processi e la documentazione rilevanti ai fini di una certificazione secondo la nuova versione. Switch trae vantaggio dal fatto che molti dei nuovi temi richiesti dalla norma sono già trattati con successo da anni: ad esempio le informazioni sulle minacce attraverso il CERT o le soluzioni di sicurezza proprie come il DNS firewall. La certificazione indipendente attesta che Switch ha implementato con successo ed efficacia un sistema di gestione della sicurezza dell'informazione. Ciò garantisce che Switch adempie ai propri compiti di gestione delle infrastrutture critiche e di protezione dei dati personali anche ai sensi della LPD e della LSIIn.

Novità pianificate 2024

Web crawler per il registry

Per contrastare malware e phishing, il registry dipende dalle segnalazioni dei servizi specializzati. Fino alla fine del 2023 l'NCSC ha gestito un web crawler che interrogava singolarmente i server web della zona .ch e analizzava le risposte alla ricerca di pattern sospetti. In caso di sospetto di malware o phishing, l'NCSC notificava le segnalazioni a Switch. Noi esaminavamo le pagine con i nostri strumenti e, in caso di sospetto confermato, attivavamo i processi corrispondenti per rimuovere le pagine web dalla rete o far rimuovere il codice dannoso.

Con l'eliminazione del crawler NCSC, al registry manca un input importante per la lotta alla criminalità informatica. Per questo motivo Switch ha sviluppato già alla fine dell'autunno un proprio crawler per le zone .ch e .li. Switch ha le fonti commerciali e informali necessarie per i pattern, senza le quali il crawler sarebbe inutile.

La messa in funzione è prevista il prima possibile, preferibilmente già a gennaio o febbraio 2024.

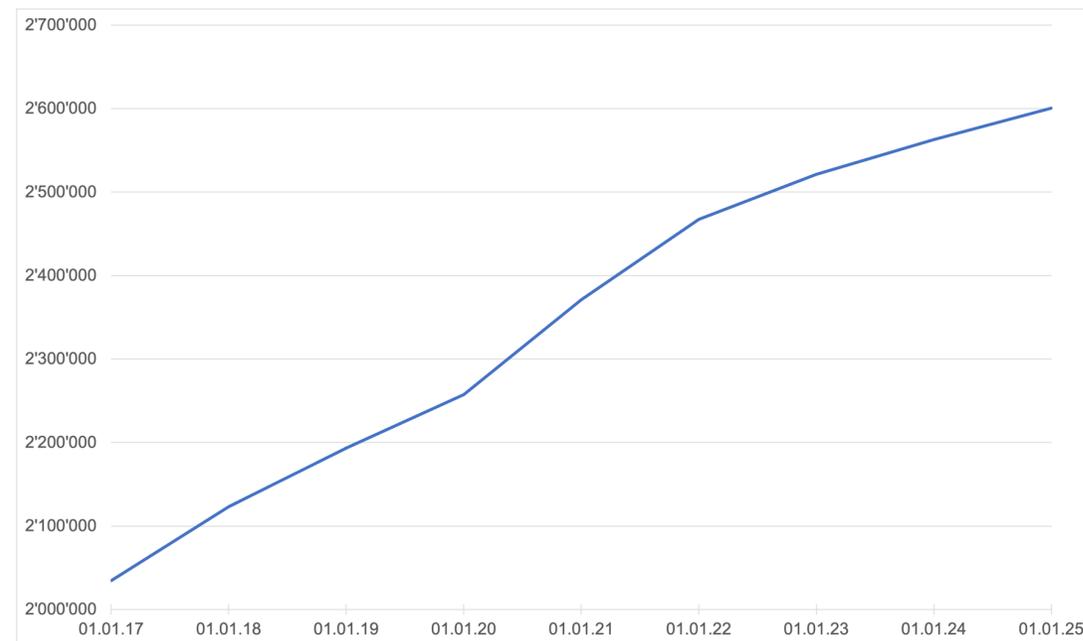
Previsione di crescita per i nomi a dominio .ch

Il 2018 e il 2019 hanno registrato un aumento, che è calato leggermente di anno in anno. Nel 2020, la spinta alla digitalizzazione dovuta alla pandemia e le iniziative di marketing dei hosting provider hanno portato a un aumento della domanda e quindi a una crescita del 4.8%. L'aumento è sceso al 3.9 % già nel 2021, rimanendo comunque più elevato rispetto a prima della pandemia.

Per il 2022 il registry ha segnato ancora una crescita del 2.1%. La spinta alla digitalizzazione è durata quindi due anni e si è tradotta in una crescita inaspettata di circa 100'000 nomi a dominio.

Nel 2023 la crescita si è attestata a oltre 40'000 nomi a dominio, che corrisponde all'1.6% e non raggiunge la nostra previsione dell'1.8%.

Stiamo assistendo a una saturazione del mercato e a una crescita contenuta a livello globale dei nomi a dominio. La nostra previsione per il 2024 conta su un aumento dell'1.45%.



Switch

Werdstrasse 2
Casella postale
CH-8021 Zurigo

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