# Sicherheit im Internet

Trends, Gefahren, Strategien

SWITCH

# Internetlandschaft: Die Schweiz digitalisiert sich mit Highspeed

Über das Internet können viele Prozesse einfacher, schneller und kostengünstiger abgewickelt werden als auf physischem Weg. Deswegen treibt der Bund die Versorgung der Schweiz mit Highspeed-Internet voran. Im Jahr 2013 verfügten hierzulande 91 Prozent der Haushalte über einen Internetanschluss. Damit gehört die Schweiz zu den besterschlossenen Ländern weltweit.

Parallel dazu verlegt der Bund unter dem Stichwort E-Government immer mehr Teile der Verwaltung und des öffentlichen Bereichs aufs Netz. So sieht der Schwerpunktplan 2016–2019 vor, dass die Schweizer Bevölkerung bis 2019 den Umzug, die Wahlen und Abstimmungen sowie die Mehrwertsteuer elektronisch abwickeln kann.

# Gefahrenlandschaft: Die Schattenwirtschaft profitiert

Die fortschreitende Verlagerung von Verwaltungs- und Geschäftsprozessen ins Internet ruft kriminelle Profiteure auf den Plan: Cybercrime hat sich in den letzten Jahren zu einem ernst zu nehmenden, sehr lukrativen Wirtschaftszweig entwickelt. Denn das Risiko, im virtuellen Raum erwischt zu werden, ist vergleichsweise gering. In einer Studie aus dem Jahr 2014 kommt das Center for Strategic and International Studies in Washington zum Schluss, dass Cyberattacken weltweit Schäden in der Höhe von insgesamt 375 bis 575 Milliarden US-Dollar pro Jahr verursachen. Im Vergleich dazu: Das Bruttoinlandprodukt der Schweiz betrug im Jahr 2013 umgerechnet 686 Milliarden US-Dollar.

# Cybercrime ist diversifiziert

Bevorzugten Internetverbrecher früher Banken für ihre Aktivitäten, so sind ihre Interessen heute breiter gefächert. Aktuell stehen bei ihnen der Software- und Technologiesektor, Unternehmens- und Beratungsservices, den Einzelhandel, das Bau- und Ingenieurwesen sowie neu auch staatliche Organisationen im Fokus.

# Wie die Ziele ausgewählt werden

Zwei Dinge ziehen die Cyberkriminellen besonders an: grosse Gewinne und kleine Aufwände. Für Erstere setzen die Täter manchmal sogar Advanced Persistent Threats (APT) ein, also aufwendige Methoden, die für das Ziel massgeschneidert worden sind. War APT früher eine Spionagemethode, dient sie heute auch monetären Zielen. Für Zweitere ist im Internet vergleichsweise preisgünstige, beliebig einsetzbare Schadsoftware erhältlich. Ein Beispiel ist das Toolkit Tinba, das die Schweizer Banken 2015 in Atem hielt. Es kostet nur wenige Tausend Franken.

**375 – 575 Mia.**

US-Dollar beträgt der weltweite Schaden, der jährlich durch Cyberkriminalität entsteht. Dies schätzt das Center for Strategic and International Studies in Washington.

**439 Mio.**

Varianten von Schadprogrammen existieren derzeit gemäss dem deutschen Bundesamt für Sicherheit in der Informationstechnik. Die Zahl steigt rasant an, weil die Programme teils automatisch generiert werden.

**205**

Tage vergehen laut der Sicherheitsfirma Mandiant im Durchschnitt, bis nach den ersten Spuren ein APT-Angriff wirklich festgestellt werden kann. Manchmal dauert es aber auch mehrere Jahre.

# .ch – eine der sichersten Domains der Welt

In der Schweiz können wir uns glücklich schätzen: .ch gehört zu den sichersten Domains der Welt, wie unterschiedliche Studien belegen. Das ist kein Zufall, sondern das Resultat gut organisierter und stets optimierter Anstrengungen. Die .ch-Registry verfügt über eingespielte Abläufe, langjährige Vertrauensbeziehungen sowie über lange Zeit aufgebaute Expertise. Und das Ziel muss nun sein, das hohe Sicherheitsniveau der .ch-Domain zu halten.

# Pionierhaft: Bekämpfung von Domainmissbrauch per Gesetz

Das Herzstück der Sicherheitsanstrengungen um die .ch-Toplevel-Domain ist auf jeden Fall der Malwareprozess. In seiner Art ist er bisher weltweit einmalig. Es handelt sich dabei um ein effizientes, gut eingespieltes, gemeinsames Vorgehen gegen die Internetkriminalität zwischen SWITCH, den Behörden und den Registraren. Seit 2010 ist dieses Vorgehen gesetzlich verankert. Artikel 15 der Verordnung über Internet-Domains (VID) lässt eine schnelle Reaktion bei Missbrauchsverdacht zu: Wenn auf einer .ch-Website Malware gemeldet wird, benachrichtigt SWITCH die Inhaber der Domains mit den verseuchten Websites. Reagieren diese nicht innerhalb eines Werktages, deaktiviert SWITCH die entsprechenden Domain-Namen. Damit sind die verseuchten Websites von aussen nicht mehr zugänglich und können keine Viren, Trojaner oder andere Schadsoftware mehr verbreiten. Die Deaktivierung ist gemäss VID während fünf Werktagen möglich.

# Eingespielte Zusammenarbeit mit den Behörden

Nur auf Antrag einer vom BAKOM akkreditierten Behörde kann die Deaktivierung verlängert werden. Andernfalls muss SWITCH die Website nach Ablauf der Frist wieder aufschalten. Aber wir von SWITCH überprüfen nun die Identität des Halters und übergeben den Fall den Behörden. Falls der Domainhalter innerhalb der nächsten 30 Tage weder die schädlichen Inhalte entfernt noch seine Identität nachweist, löscht SWITCH den betroffenen Domain-Namen endgültig. Dieses konsequente Vorgehen macht .ch-Domains für die Verbreitung von Malware unattraktiv, da Cyberkriminelle hier für ihr Ansinnen einen grossen Aufwand betreiben müssen.

## Art. 15 VID

ist das Herzstück des Kampfes gegen die Internetkriminalität in der Schweiz. Er lässt eine schnelle Unterbindung von Attacken auf Websitebesucher in der Schweiz zu.

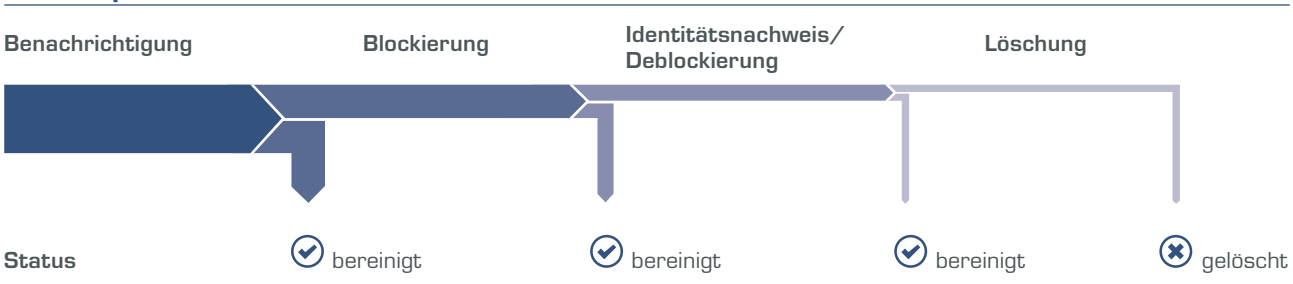
## Einzigartig

.ch ist weltweit die einzige Registry, die koordiniert mit dem Regulator und mit Partnern gegen Malware vorgeht. Der Erfolg gibt dem Vorgehen recht: Die Toplevel-Domain gehört zu den sichersten der Welt.

## Unattraktiv

ist .ch für Internetkriminelle. Es wird für Letztere zu teuer, immer wieder Ersatz für Domains zu finden, die wegen Malwareverbreitung gelöscht oder vom Schadcode befreit wurden.

**Malwareprozess**



# Erster Rang für .ch in Sachen Sicherheit

Wie erwähnt, ziehen unter anderem kleine Aufwände die Schattenwirtschaft an. Wenn Cyberkriminelle Toplevel-Domains für ihre Machenschaften suchen, so sind für sie besonders solche attraktiv, die über tiefe Preise und eine offene Registrierungs-Policy verfügen. .ch wäre damit äusserst attraktiv für Internetkriminalität, denn beide Kriterien treffen für diese Toplevel-Domain zu. 2015 untersuchte die auf Internet-Analysen spezialisierte US-Firma Architelos den Missbrauch auf Webseiten (Malware und Phishing) in Europa und ordnete diesen den einzelnen Toplevel-Domains zu. Dabei belegte .ch bezüglich Sicherheit den ersten Platz. Also kann man schliessen, dass dies den Sicherheitsanstrengungen bei .ch zu verdanken ist. Das Ziel muss nun lauten, das hohe Sicherheitsniveau der Registry in der Schweiz zu halten und die Sicherheitsmassnahmen stets den dynamischen Bewegungen der Cybercrime-Wirtschaft anzupassen.

# Sicherheit bei SWITCH: ISO-zertifiziert und preisgekrönt

Die Sicherheit der .ch-Registry ist eine Kernaufgabe von SWITCH. Wir von SWITCH verfügen über ein etabliertes Informationssicherheits-Managementsystem (ISMS). Damit wird die Sicherheit ständig kontrolliert und optimiert. 2014 haben wir dafür die ISO-27001-Zertifizierung bekommen. Wir arbeiten mit unseren Pendants in Österreich und Deutschland zusammen und überprüfen gegenseitig die Sicherheitsabläufe unserer Registrys. Im Oktober 2015 haben wir deswegen den CENTR-Sicherheitspreis gewonnen. CENTR, der Council of European National Toplevel Registries, ist die europäische Vereinigung der Registrierungsstellen für Toplevel-Domains.

## CENTR

Der Council of European National Toplevel Registries hat SWITCH im Oktober 2015 mit seinem Sicherheitspreis ausgezeichnet.

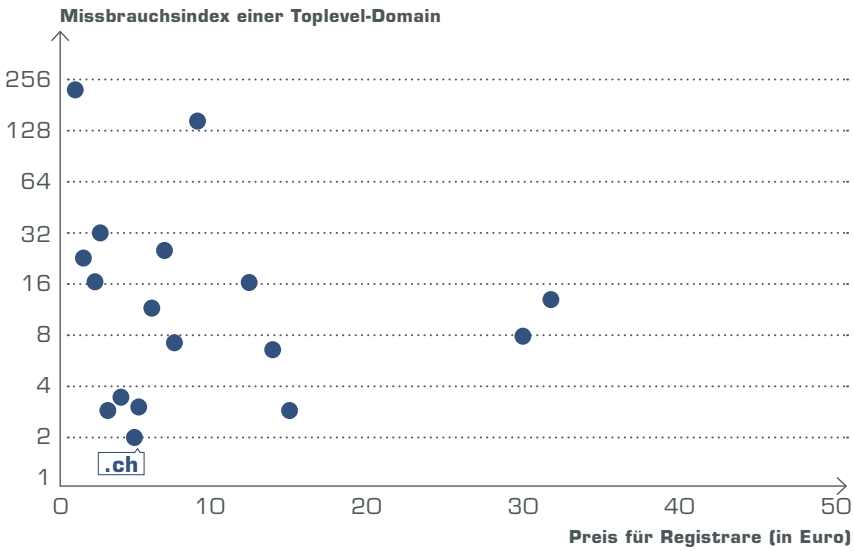
## DNSSec

Die kryptografischen Schlüssel für .ch werden bei SWITCH in der Schweiz gehostet. Es handelt sich dabei um Signaturen für die sicheren und schwer angreifbaren https-Domains.

## ISO-27001

ist das Zertifikat für ein Informationssicherheits-Managementsystem (ISMS), über das die .ch-Registry verfügt. SWITCH optimiert ihr ISMS stetig.

**Preis- Sicherheits-Verhältnis europäischer Registrys**




● Europäische Registry mit offener Policy

Die Darstellung zeigt: Unter den europäischen Registrys mit offener Policy belegt .ch den ersten Platz bezüglich Sicherheit.

Zahlenmaterial: Architelos; die Registrys sind aus Gründen der Vertraulichkeit anonym.

# Hilfe für Betreiber von gehackten Websites

Meistens sind Website-Betreiber selber überrascht, wenn ihre Websites schädliche Inhalte verbreiten. Sie sind Opfer cyberkrimineller Machenschaften. SWITCH gibt ihnen Anweisungen, wie sie die Malware entfernen können. Im Jahr 2015 stellte SWITCH in 761 Fällen Malware auf .ch-Websites fest. In den meisten Fällen, nämlich in 556 davon, entfernten die Domain-Halter den schädlichen Code gleich nach der ersten Benachrichtigung.

# Strategie gegen Phishing

Phishing bezeichnet Versuche, illegal an vertrauliche Informationen zu gelangen. SWITCH identifizierte 2015 insgesamt 320 solcher Fälle. Aufgrund der rasanten Zunahme von Phishing-Fällen weltweit hat SWITCH den Malwareprozess 2014 um die Bekämpfung von Phishing erweitert. Mit Erfolg: Momentan beobachten wir von SWITCH auf .ch keine Zunahme der Phishing-Fälle.

# Sicherheit als Mission

Zugunsten einer sauberen .ch-Toplevel-Domain muss die Schweizer Bevölkerung über die Gefahren aus dem Cyberspace aufgeklärt werden. Sie muss wissen, wie sie sich effizient schützen kann. Deswegen hat SWITCH 2014 die Swiss Internet Security Alliance (SISA – www.swiss-isa.ch) mitbegründet. In ihr sind wichtige Player aus der Telekommunikations- und Internetbranche zusammengeschlossen mit dem Ziel, die Schäden zu reduzieren, die durch Internetkriminalität entstehen. Ausserdem haben wir von SWITCH die Aufklärungsseite www.switch.ch/safer-internet aufgeschaltet mit Tipps zum Schutz vor Attacken.

**761**

Fälle von Malwareverbreitung auf Websites stellte SWITCH 2015 fest.

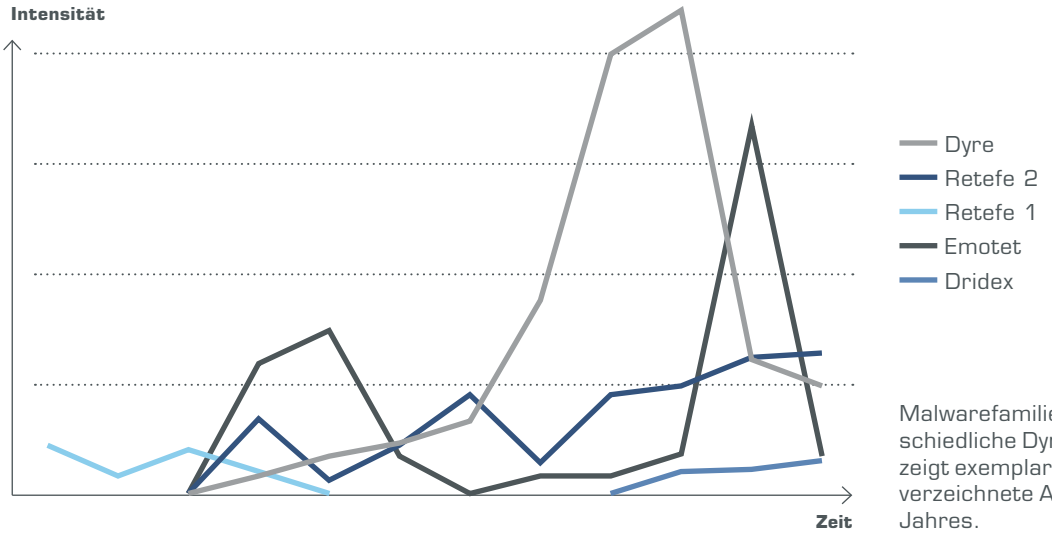
**320**

Fälle von Phishing stellte SWITCH 2015 fest. In 53 davon hat SWITCH die Domain blockiert. SWITCH will verstärkt gegen Phishing vorgehen, in Zusammenarbeit mit internationalen Partnern.

**SISA**

wurde von SWITCH mitbegründet. In der Swiss Internet Security Alliance sind wichtige Player aus der Schweizer Telekommunikations- und Internetbranche im Kampf gegen Cybercrime zusammengeschlossen.

**Malware und ihre Dynamik**




Malwarefamilien entfalten unterschiedliche Dynamiken. Die Grafik zeigt exemplarisch in der Schweiz verzeichnete Attacken während eines Jahres.

# Wie SWITCH zu ihren Informationen kommt

Ganz wichtig für die Beseitigung von Schadsoftware ist es, dass man weiss, welche .ch-Websites verseucht sind. Wir von SWITCH verfügen über diese Informationen, weil wir Teil eines weltweiten Alarmierungs- und Wissensaustauschnetzwerks sind. In dieser privilegierten Lage sind wir, weil wir nicht nur Betreiberin der .ch-Registry sind, sondern auch über ein CERT (Computer Emergency Response Team) verfügen, und zwar bereits seit 1991. Wir sind somit die Organisation in der Schweiz, die über die längste Erfahrung mit der Bekämpfung von Cyberbedrohungen verfügt. Das CERT von SWITCH ist international renommiert. Wir bekommen Anfragen aus der ganzen Welt, beim Aufbau von CERTs behilflich zu sein. SWITCH-Mitarbeitende erteilen zudem weltweit Unterricht in der Bekämpfung von Cybercrime.

SWITCH ist unter anderem Mitglied folgender Organisationen:
→ FIRST (weltweite Dachorganisation aller CERTs)
→ TF-CSIRT (Verbund europäischer CERTs)
→ MELANI-Net (Plattform der Melde- und Analysestelle Informationssicherung des Bundes)
→ SISA (Swiss Internet Security Alliance; Gründungsmitglied)

# Die zweite Informationsquelle: Der Backbone

Die Partnerorganisationen sind jedoch nicht die einzige Quelle für Informationen über verdächtige Machenschaften im Internet. SWITCH ist auch Betreiberin des Internet-Backbones der Schweizer Hochschulen. Dabei versorgen wir diese nicht nur mit modernsten Internetdienstleistungen. Wir beobachten auch deren externen Netzwerkverkehr auf Anomalien. Diese Informationen analysieren wir und korrelieren sie einerseits mit weiteren eigenen Quellen, anderseits mit jenen von Partnern. Dadurch verfügen wir über ein detailliertes Bild der aktuellen lokalen Bedrohungslage und der Trends.

# Erfahrungen zugunsten der ganzen Schweiz

Als Attackenziel der ersten Stunde nehmen Banken seit Jahren Sicherheitsdienstleistungen von SWITCH in Anspruch. Die Erfahrung mit der Domäne der Finanzdienstleistungen erweitert den Know-how-Horizont von SWITCH und kommt letztlich der gesamten Schweizer Öffentlichkeit zugute.

## 1991

wurde das CERT (Computer Emergency Response Team) von SWITCH gegründet. Es ist das älteste der Schweiz.

## Vertrauen

SWITCH tauscht mit Partnern weltweit Informationen über verdächtige Machenschaften im Internet aus. Die Beziehungen setzen Vertrauen voraus und sind über Jahre aufgebaut worden.

## Backbone

Wir von SWITCH betreiben den Internet-Backbone der Schweizer Hochschulen. Wir schützen deren Netzwerkverkehr.

# Über SWITCH

SWITCH ist eine Stiftung, die vom Bund und den Hochschulkantonen gegründet wurde. Als solche ist sie unabhängig, neutral und nicht gewinnorientiert. Sie wurde 1987 ins Leben gerufen, um den Hochschulen ICT-Dienstleistungen anzubieten. Es war auch SWITCH, die die Schweiz 1990 in dieser Funktion ans Internet angeschlossen hat.

Die Öffentlichkeit kennt SWITCH als Registrar der ersten Stunde von .ch-Internet-Domains. Aufgrund einer Änderung in der Verordnung über Internet-Domains (VID) haben wir von SWITCH diese Funktion im Verlauf des Jahres 2015 schrittweise an die Registrare abgegeben. Die Datenbank mit den Domain-Namen, die Registry, führen wir im Auftrag des Bundesamtes für Kommunikation (BAKOM) weiter. Sie ist gemäss Bundesrat eine kritische Infrastruktur. Fiele sie aus, wäre die Kommunikation übers Internet unterbrochen. Damit kämen wesentliche Teile des öffentlichen Lebens in der Schweiz praktisch zum Erliegen. Uns wurde vom Bundesamt für wirtschaftliche Landesversorgung (BWL) attestiert, dass wir diese Infrastruktur optimal betreiben und schützen.

**1987**
wurde SWITCH gegründet.

**1990**
hat SWITCH die Schweiz ans Internet angeschlossen.

**Neutral**
SWITCH ist aufgrund ihrer rechtlichen Struktur als Stiftung unabhängig, neutral und nicht gewinnorientiert.

# Was SWITCH auszeichnet

→ **Pioniere:** Wir haben das Internet vor bald 30 Jahren in die Schweiz gebracht und kennen es von Grund auf. Wir haben die .ch-Registry selbst aufgebaut. Kaum jemand hat diesbezüglich so viel Know-how wie wir.

→ **Eingespielte Prozesse mit Behörden und Internet-Providern:** Über all die Jahre haben wir eine gute Zusammenarbeit mit den Behörden wie dem BAKOM und der Strafverfolgung sowie den Registraren etabliert und kennen deren Bedürfnisse. Zusammen haben wir .ch zu einer der sichersten Toplevel-Domains der Welt gemacht.

→ **Internationales Sicherheitsnetzwerk:** Wir verfügen seit 25 Jahren über ein eigenes, weltweit renommiertes Computer Emergency Response Team (CERT) und ein entsprechendes Netzwerk im In- und Ausland. Unsere langjährigen Vertrauensbeziehungen kommen uns bei der Bekämpfung von Cyberkriminalität zugute. Es braucht Jahre, bis solche Vertrauensbeziehungen aufgebaut sind.

→ **Kritische Infrastruktur:** Wir betreiben mit dem DNS eine kritische Infrastruktur, die bis heute stabil und verlässlich läuft. Aber auch in einem nationalen Krisenfall können wir garantieren, dass der Dienst unter Schweizer Kontrolle weiterfunktioniert, da die Kerninfrastruktur in der Schweiz betrieben wird.

SIDEF 1 2016, Coverphoto: Frank Bruederli

Das Ziel muss sein, das hohe Sicherheitsniveau der .ch-Domain zu halten.

SWITCH
Werdstrasse 2
Postfach
CH-8021 Zürich

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