



28.8.2017

Revision der Verordnung über Internet-Domains (VID)

Erläuterungsbericht

Die Revision der Verordnung über Internet-Domains (VID; SR 784.104.2) ist notwendig, um die regulatorischen Rahmenbedingungen zur Bekämpfung der Cyberkriminalität anzupassen und dabei den Erfahrungen aus eineinhalb Betriebsjahren der Domain .swiss Rechnung zu tragen.

Art. 10 Abs. 1 Bst. j und k Aufgaben

Die Registerbetreiberinnen von .ch und .swiss mussten bis anhin nicht nur eine Liste der Registrare veröffentlichen (Art. 18 Abs. 1 VID), sondern auch ein Verzeichnis der Registrare zur Verfügung stellen, das nach gewünschten Dienstleistungen durchsucht werden kann (Art. 10 Abs. 1 Bst. j VID in fine) und mit dem die Registrare mit Domain-Namen zusammenhängende Dienste auswählen und ihrem Profil hinzufügen können (Bst. k). Diese letzte Dienstleistung der Registerbetreiberinnen (Art. 10 Abs. 1 Bst. j VID in fine und Bst. k) hat sich als überflüssig erwiesen und wird gestrichen, da sie nicht den Bedürfnissen der Registrare entspricht und gemäss den international angewendeten Regeln nicht erforderlich ist. Zudem hat sie sich in der Praxis nicht bewährt.

Art. 14 Abs. 4 Streitbeilegungsdienste

Die Entscheide der Streitbeilegungsdienste betreffen zivilrechtliche Streitigkeiten zwischen Halterinnen und Haltern von Domain-Namen und Inhaberinnen und Inhabern von Kennzeichenrechten wie Firmen, Namen, geschützte geografische Bezeichnungen oder Marken (vgl. Art. 14 Abs. 1 Bst. b VID). Solche Streitigkeiten und die Legitimität derer können oft nur verständlich wiedergegeben werden, wenn die Identität der Parteien bekannt ist. Diese ist nämlich oft der massgebende Faktor, der die entsprechenden Rechte begründet oder ihnen entgegensteht. Mit anderen Worten kann die Veröffentlichung von Entscheiden der Streitbeilegungsdienste ohne klare Identifikation der beteiligten Parteien wertlos sein. Diese Tatsache rechtfertigt, das in Artikel 14 Absatz 4 VID vorgesehene grundsätzliche Verbot, Namen und andere persönliche Angaben der Parteien zu publizieren, aufzuweichen.

Art. 15 ff. Massnahmen bei Missbrauchsverdacht

Eine wirksame Bekämpfung von Missbräuchen, die mithilfe von schweizerischen Domain-Namen .ch und .swiss betrieben wird, trägt zur Gewährleistung der Sicherheit im Internet bei und verstärkt das Vertrauen der Nutzerinnen und Nutzer in die online auf diesen Domains verfügbaren Inhalte und Dienste. Die Bekämpfung der Cyberkriminalität ist in diesem Zusammenhang eine der wichtigsten Aufgaben einer Registerbetreiberin (Art. 10 Abs. 1 Bst. i VID). Vor allem die in Artikel 15 VID vorgesehenen Massnahmen und Verfahren bilden seit ihrer Einführung im Jahr 2010 das Fundament der Bekämpfung bestimmter spezifischer Cyberdelikte (Phishing und Verbreitung von schädlicher Software [Malware]), die mithilfe von Websites oder Webdiensten über Schweizer Domain-Namen verübt wer-

den. Diese Regelungen und Verfahren haben sich als wirksam erwiesen und machen die Schweizer Internet-Domains zu den sichersten der Welt. Insgesamt sind seit 2010 über 11'400 Malware- und mehr als 1'110 Phishing-Fälle in der .ch-Domain festgestellt und behandelt worden (Statistiken von SWITCH Ende Dezember 2016; statistische Daten bezüglich Phishing erst seit 2014). Für die .swiss-Domain ist bisher noch kein Missbrauchsfall verzeichnet worden (Öffnung im September 2015).

Aufgrund der gesammelten Erfahrungen und der raschen Weiterentwicklung der Praktiken und Vorgehensweisen der Cyberkriminellen sowie der Überlegungen, die derzeit in der für die weltweite Verwaltung des Domain-Namen-Systems (DNS) zuständigen internationalen Organisation (d. h. der Internet Corporation for Assigned Names and Numbers [ICANN]) in Bezug auf Bekämpfung der Cyberkriminalität angestellt werden, müssen einige Bestimmungen abgeändert werden. Mit diesen Änderungen soll die Bekämpfung der Cyberkriminalität und deren Wirksamkeit ausgeweitet und verbessert werden.

Art. 15 Massnahmen bei Missbrauchsverdacht: Blockierung

Unter Artikel 15 VID fallen lediglich die Tatbestände des Phishings und der Verbreitung schädlicher Software, da bei diesen beiden Handlungen Domain-Namen verwendet werden. Eine derartige Nutzung von Domain-Namen kann verschiedenste Formen annehmen und durch unterschiedlichste Techniken erfolgen. Dabei werden verschiedene Mittel eingesetzt: Netzwerke mit Zombie-Geräten (Botnets), Massenversand von E-Mails (Spam), das Ausnutzen technischer Schwachstellen einer Website ohne Wissen des Betreibers, das Klonen von Websites oder die Manipulation des DNS zur Umleitung auf gefälschte oder geklonte Websites (Pharming). Die Methoden für Phishing-Aktivitäten und Malware-Verbreitung über Domain-Namen entwickeln, vervielfachen und diversifizieren sich rasch und in hohem Mass. Deshalb muss Artikel 15 Absatz 1 VID dahingehend ergänzt werden, dass nicht nur die Verbreitung von Malware, sondern auch deren Nutzung erfasst wird (Bst. b). So können Domain-Namen von Websites ins Visier genommen werden, die Befehle für Botnets übertragen (Steuerungs- und Kontrollserver eines Botnets oder "Command & Control server" [C&C-Server]). Letztere greifen dabei oft auf Domain-Generation-Algorithmen (DGA) zurück, um die Spuren zu verwischen. Ausserdem ist es angezeigt, einen neuen Buchstaben c einzuführen, damit die Regelungen von Artikel 15 VID in allen Fällen angewendet werden können, in denen ein Domain-Name direkt oder indirekt („unterstützen“) für Phishing oder die Verbreitung von Malware eingesetzt wird. So soll der raschen und unvorhersehbaren Entwicklung der Mittel, Techniken und Vorgehensweisen der Cyberkriminellen entgegengewirkt werden können. Der neue Buchstabe c deckt beispielsweise jene Fälle ab, in denen Domain-Namen zusammen mit Social-Engineering-Praktiken als Köder zu Phishing-Zwecken eingesetzt werden, wenn Domain-Namen mit DGA generiert werden oder wenn zur Unterstützung böswilliger Handlungen konfigurierte Server benutzt werden.

Die Registerbetreiberin kann ohne Antrag einer zur Bekämpfung der Cyberkriminalität anerkannten Stelle (Abs. 3) einen Domain-Namen für höchstens fünf Werkzeuge technisch und administrativ blockieren, wenn die Voraussetzungen dafür erfüllt sind (Abs. 1). Nach Ablauf dieser Frist muss die Registerbetreiberin jede Blockierungsmassnahme aufheben, die nicht durch eine anerkannte Stelle (Abs. 3) oder eine Anordnung des Bundesamtes für Polizei (fedpol) (Abs. 4) bestätigt wird. Die Registerbetreiberin kann die fünftägige technische und/oder administrative Blockierung gemäss Absatz 1 aus eigenem Anlass nur verlängern, wenn der begründete Verdacht besteht, dass die Halterin oder der Halter offensichtlich falsche Identifizierungsangaben macht oder unrechtmässig die Identität eines Dritten verwendet, und die zeitliche Dringlichkeit besteht, einen drohenden, nicht leicht wiedergutzumachenden Nachteil abzuwenden (Abs. 2). Neben dieser Bestimmung kann eine Schweizer Behörde, die im Rahmen ihrer Zuständigkeit interveniert, jederzeit die Blockierung eines Domain-Namens beziehungsweise die Verlängerung der Blockierung gestützt auf Artikel 30 Absatz 3 Buchstabe a VID verlangen.

Gemäss Absatz 3 kann eine anerkannte Stelle wie MELANI nicht nur eine vollständige technische Blockierung bestätigen, sondern auch von der Registerbetreiberin verlangen, dass die vorgängig in der Zonendatei gelöschten Namensserver nicht wieder eingefügt werden (vgl. die neue Fassung von Art. 30 Abs. 3 Bst. a VID). Die Verbindung zum Domain-Namen und folglich die mutmassliche Verbreitung von Malware bleibt unterbrochen. Dieses pragmatische Vorgehen ermöglicht es, eine Blockie-

nung im Interesse der öffentlichen Sicherheit aufrecht zu erhalten, wenn Zweifel darüber bestehen, ob der Domain-Name zu Phishing oder Malwarezwecken benutzt wird..

. Ein zu schnell blockierter Domain-Name bzw. gelöschter Namensserver kann daher auch wieder eingefügt werden, wenn sich der Verdacht nicht bestätigt hat.

Art. 15a Massnahmen bei Missbrauchsverdacht: Umleitung des Datenverkehrs

Die aktuelle, in Artikel 15 VID vorgesehene Regelung zur Bekämpfung der Cyberkriminalität muss mit der Möglichkeit ergänzt werden, den Datenverkehr zu Domain-Namen, die für Phishing oder Malware-Verbreitung verwendet werden, zu Analysezwecken umzuleiten ("domain name traffic sinkholing"). Eine solche Massnahme verbessert die Bekämpfung dieser Art von Cyberkriminalität deutlich, da sie es ermöglicht, die infizierten Server / Computer ausfindig zu machen, die Opfer zu informieren und die Funktionsweise dieser Aktivitäten zu analysieren. So können Techniken zur Bekämpfung solcher krimineller Handlungen entwickelt und Hinweise gesammelt werden, um mehr über die Bedrohung zu erfahren. Damit kann allfälligen künftigen Handlungen entgegengewirkt werden. Diese ebenfalls von der ICANN im Kampf gegen die Cyberkriminalität empfohlene Massnahme kann die Registerbetreiberin einfach umsetzen, da sie die mit einem Domain-Namen verbundenen Namensserver in der Zonen-datei durch neue Namensserver ersetzen kann, die so eine Umleitung des Datenverkehrs ermöglichen (vgl. auch Art. 30 Abs. 3 Bst. b VID und entsprechende Erläuterungen zu Art. 30 VID). Da diese Massnahme die Bearbeitung von über den Fernmeldeweg übermittelten Informationen und Korrespondenzen umfasst, die ursprünglich für Dritte bestimmt waren, muss sie eingegrenzt werden. In Artikel 15a VID wird daher festgelegt, unter welchen Voraussetzungen eine Sinkholing-Massnahme erlaubt ist:

- Der zu einem Domain-Namen führende oder über diesen geführten Datenverkehr kann nur umgeleitet werden, wenn der Domain-Name im Sinne von Artikel 15 VID technisch und administrativ blockiert ist (Bst. a).
- Die Analyse des Datenverkehrs darf einzig dazu dienen, die Phishing- und Malware-Opfer zu identifizieren, sie zu informieren sowie die Funktionsweise zu analysieren, damit Techniken entwickelt werden können, die das Erkennen, Bekämpfen, Beschränken oder Nachverfolgen solcher Handlungen ermöglichen. Die gesammelten und analysierten Informationen, die nicht für diesen Zweck vorgesehen sind, müssen unmittelbar und definitiv gelöscht werden (Bst. b).
- Nur eine zur Bekämpfung der Cyberkriminalität anerkannte Stelle und fedpol können bei der Registerbetreiberin die Umleitung des Datenverkehrs zu Analysezwecken verlangen, wobei Erstere die Umleitung für höchstens 30 Tage beantragen kann (Bst. c; vgl. auch Art. 30 Abs. 3 Bst. g VID betreffend die Behörden, die im Rahmen ihrer Zuständigkeit intervenieren). Die Bearbeitung der umgeleiteten Informationen erfolgt a priori durch die anerkannte Stelle oder die zugezogene Behörde. Diese Letzteren dürfen, die Analyse entweder der Registerbetreiberin oder Dritten zu übertragen, wenn diese für ihre Kompetenzen und ihr Know-how in diesem Bereich anerkannt sind ("Security Research Partner", Stelle für forensische Untersuchungen oder anderer "Quarantäneregistrar" ["quarantine registrar"]). Derjenige, der die Umleitung des Verkehrs zu Analysezwecken verlangt, bleibt allerdings für die Bearbeitung der gesammelten Informationen verantwortlich und muss dafür sorgen, dass er und allfällige Beauftragte die für diese Bearbeitung gemäss Artikel 15a VID geltenden Voraussetzungen erfüllen.
- Die einschlägigen Informationen und die Analysen, die zur Bekämpfung der Cyberkriminalität dienen, können gemäss Artikel 16 Absätze 1, 2 und 4 VID zwischen Behörden, spezialisierten Bundesstellen und anderen Dritten, die bei der Feststellung und Beurteilung von Bedrohungen, Missbräuchen und Gefahren mitarbeiten, ausgetauscht werden.

Art. 15b Massnahmen bei Missbrauchsverdacht: Information und Antrag auf Identifikation

Die Halterin oder der Halter eines Domain-Namens, der blockiert oder dessen Datenverkehr umgeleitet worden ist, muss umgehend über eine solche Massnahme informiert werden (Abs. 1). Diese Information kann zu einem späteren Zeitpunkt erfolgen, wenn es zum Schutz von überwiegenden öffentlichen oder privaten Interessen erforderlich ist (Abs. 3). Dies ist insbesondere dann der Fall, wenn die Information dazu führen würde, die mutmasslich Phishing- oder Malware-Angriffe verübende Person vor einer gegen sie ergriffenen Massnahme zu warnen, welche jedoch gerade darauf abzielt, die Betrugshandlungen zu verhindern oder zu bekämpfen.

Alle Massnahmen im Sinne der Artikel 15 und 15a VID werden ausserdem in der Regel mit der Forderung verbunden, die Identität bekannt zu geben und/oder eine Korrespondenzadresse in der Schweiz zu bezeichnen (Abs. 2).

Art. 15c Massnahmen bei Missbrauchsverdacht: Verfügung und Widerruf

fedpol erlässt eine Verfügung über die Blockierung und/oder die Umleitung des Datenverkehrs, wenn die Halterin oder der Halter innerhalb von 30 Tagen nach der sofortigen oder späteren Mitteilung der Massnahme durch die Registerbetreiberin eine solche Verfügung verlangt, ihre oder seine Identität korrekt bekannt gibt und eine gültige Korrespondenzadresse in der Schweiz bezeichnet, falls ihr oder sein Sitz oder Wohnsitz im Ausland liegt (Abs. 1).

Die Forderung nach der Bezeichnung einer Korrespondenzadresse in der Schweiz ("Rechtsdomizil") oder der Bekanntgabe der Identität im Sinne von Artikel 15b Absatz 2 VID spielt eine wesentliche Rolle im Kampf gegen Cyberkriminalität. Sie ergänzt die zeitlich begrenzten Blockierungsmassnahmen nach Artikel 15 VID und bietet auf einfache und wirksame Weise die Möglichkeit, die für unerlaubte Handlungen verwendeten Domain-Namen endgültig zu widerrufen. Letztere werden nämlich oft unter Angabe einer falschen Identität erworben, um die Anonymität des Internets auszunützen. Diese Halterinnen und Halter werden mit hoher Wahrscheinlichkeit einem Identifizierungsbegehren nie nachkommen.

Die Registerbetreiberin kann ausserdem ungeachtet der Artikel 15 ff. VID die Bekanntgabe der Identität der Halterinnen und Halter gestützt auf Artikel 29 Absatz 1 VID verlangen und Domain-Namen gemäss Artikel 30 Absatz 2 Buchstabe c VID widerrufen, wenn die Halterinnen und Halter ihren Verpflichtungen nicht innerhalb von 30 Tagen nachkommen oder ihre Identität offensichtlich falsch bekannt geben.

Art. 15d Massnahmen bei Missbrauchsverdacht: nicht zugeteilte Domain-Namen

Parallel zu Artikel 15a VID ermöglicht Artikel 15d VID der Registerbetreiberin, aus eigenem Anlass oder auf Antrag einer zur Bekämpfung der Cyberkriminalität vom BAKOM anerkannten Stelle bestimmte Massnahmen für noch nicht zugeteilte Domain-Namen zu ergreifen, welche von Cyberkriminellen registriert werden könnten. Insbesondere betroffen sind Botnets oder andere Systeme, welche Domain-Generation-Algorithmen (DGA) zur Ausübung böswilliger Handlungen verwenden. Die so generierten Domain-Namen, die je nach den gewählten Parametern zufälligen Bezeichnungen entsprechen, steuern direkt oder indirekt Botnets, um über diese illegale Handlungen auszuführen. Sie dienen zudem der Ablenkung, um Rückverfolgungen zu erschweren. Im Rahmen forensischer Gutachten über infizierte Computer ist es dank Nachkonstruktionstechniken (Reverse Engineering) möglich, die DGAs nachzubilden und daraus eine Liste mit Domain-Namen zu erstellen, die von Botnets verwendet werden könnten. Die Registerbetreiberin kann diese Namen sich selber oder einem Dritten, der als "Quarantäneregistrar" seine Mitarbeit bei der Bekämpfung der Cyberkriminalität anbietet, zuteilen (Bst. a) und sodann den zum Domain-Namen führenden oder über diesen geführten Datenverkehr zu Analysezwecken umleiten. So können Cyberbedrohungen und -attacken identifiziert, abgewendet oder abgeschwächt werden (Bst. b Sinkholing). Neben diesen Massnahmen kann die Registerbetreiberin ausserdem die Zuteilung entsprechender Domain-Namen gestützt auf Artikel 25 Absatz 2 Buchstabe c VID verweigern.

Artikel 15d VID sieht im Gegensatz zu Artikel 15a VID nebst dem generellen Erfordernis eines begründeten Verdachts, dass eine Zuteilung und Nutzung eines noch nicht zugeteilten Domain-Namens zu einem unrechtmässigen Zweck oder auf unrechtmässige Weise erfolgen könnte, keine weiteren Voraussetzungen vor. Dies rechtfertigt sich dadurch, dass die in Frage stehenden Domain-Namen noch nie zugeteilt worden sind und für sie folglich keine Halterin oder kein Halter ein Nutzungsrecht oder ein schutzwürdiges Interesse am Domain-Namen geltend machen kann.

Art. 15e Massnahmen bei Missbrauchsverdacht: Dokumentation und Bericht

Die Berichte an das BAKOM über Blockierungen müssen künftig auch die Umleitungsmassnahmen zu Analyse Zwecken enthalten ("domain name traffic sinkholing"). Da in der Praxis nicht quartalsweise, sondern monatlich und jährlich Bericht erstattet wird, muss Artikel 15e VID entsprechend angepasst und "quartalsweise" durch "periodisch" ersetzt werden. Auf jeden Fall müssen die Berichte mindestens einmal pro Quartal vorgelegt werden.

Art. 16 Amtshilfe und Zusammenarbeit

Im weltumspannenden, informellen Umfeld des Internets ist es wichtig, dass die Registerbetreiberin nicht nur mit den Behörden rasch zusammenarbeiten kann, sondern auch mit Dritten, welche Bedrohungen, die von ihr verwaltete Domains betreffen könnten, bekämpfen. In diesem Zusammenhang ist es ebenso essenziell, dass sie personenbezogene Informationen bearbeiten kann. Vor diesem Hintergrund ist Artikel 16 VID dahingehend zu ändern, dass die Registerbetreiberin den spezialisierten Bundesbehörden wie z. B. MELANI wenn nötig Zugang zu den Datenbanken betreffend die Verwaltung der betroffenen Domain verschaffen kann (insbesondere Zonendatei [vgl. Art. 10 Abs. 1 Bst. a Ziff. 2 VID]). Dies geschieht über das Abrufverfahren oder durch blockweise Übertragung von Daten (Abs. 2). Des Weiteren kann die Registerbetreiberin jeder anderen, für ihre Tätigkeit im Bereich der Bekämpfung der Cyberkriminalität anerkannten Person oder Stelle, wie z. B. solchen im Sinne von Artikel 15 Absatz 1 Buchstabe b VID (Abs. 1), personenbezogene Daten bekannt geben. Dies erfolgt im Abrufverfahren. Eine Herausgabe der Daten auf einem anderen Kommunikationsweg (v. a. E-Mail) bleibt vorbehalten.

In Absatz 3 wird aus Wirksamkeits- und Praktikabilitätsgründen der Prozess zur Bezeichnung einer Korrespondenzadresse in der Schweiz ("Rechtsdomizil", das den zuständigen Behörden die Zustellung amtlicher Mitteilungen und anderer Verwaltungs- und Gerichtsentscheide insbesondere an die im Ausland ansässigen Halterinnen und Halter ermöglicht) vereinfacht, indem der Zwischenschritt abgeschafft wird, bei dem die Registrare als Intermediäre zwischen der Registerbetreiberin und den Halterinnen oder Haltern auftreten (Abs. 3 in Verbindung mit Art. 23 Abs. 3 VID, der gestrichen wird). Die Registerbetreiberin kann auf diese Weise sofort handeln, und die Schweizer Behörden gewinnen wertvolle Zeit für die Zustellung und Umsetzung ihrer Mitteilungen, Verfügungen und anderen Massnahmen zur Bekämpfung der Cyberkriminalität. Die Abschaffung des oben genannten Zwischenschrittes ist umso mehr angezeigt, als die Registrare den Schwerpunkt ihrer Arbeit auf die kommerziellen Aspekte der Beziehungen zu den Kundinnen und Kunden legen und die Missbrauchsbekämpfung folglich etwas weniger gewichten. Dazu kommt, dass die ausländischen Registrare oft nur wenig über die in der VID vorgesehenen Verfahren in der Schweiz wissen und deren Ablauf so erschwert wird.

Art. 21 Abs. 3 Informationsaufgaben

Nur die Registrare, die einen Registrarvertrag im Sinne von Artikel 17 Absatz 1 Buchstabe b und Absatz 2 VID abgeschlossen haben, können auf das elektronische Registrierungssystem der Registerbetreiberin zugreifen. Dementsprechend können nur die Registrare formell die Zuteilung von Domain-Namen im Auftrag der gesuchstellenden Personen beantragen oder die zugeteilten Domain-Namen administrativ verwalten. Ein Registrar kann jedoch auch auf Wiederverkäufer und andere Zwischenhändler zurückgreifen, die bei an einem Domain-Namen interessierten Kundinnen und Kunden werben. Die Registrare stehen folglich nicht immer direkt mit den gesuchstellenden Personen oder den Halterinnen und Haltern in Kontakt. Sie sind aber dennoch dafür verantwortlich, den Halterinnen und

Haltern oder den Gesuchstellerinnen und Gesuchstellern unverzüglich jegliche Informationen der Registerbetreiberin weiterzuleiten oder – wie dies künftig ausdrücklich in Artikel 21 Absatz 3 VID festgehalten ist – sie übermitteln zu lassen.

In Absatz 3 wird zudem genauer festgelegt, wie die Information über den Verweigerungsentscheid der Registerbetreiberin zu erfolgen hat. Demnach muss der betreffende Registrar die abgewiesenen Gesuchstellerinnen und Gesuchsteller unverzüglich, spätestens aber drei Tage nach der grundsätzlich über das Registrierungssystem erfolgenden Mitteilung der Registerbetreiberin an den Registrar (ausnahmsweise auch auf anderem Weg [vgl. Art. 27 Abs. 3 in fine VID]) informieren. Es ist von essenzieller Bedeutung für die gesuchstellende Person, schnellstmöglich Kenntnis von der Zuteilungsverweigerung der Registerbetreiberin zu haben, da ab Zeitpunkt der Mitteilung gemäss Artikel 27 Absatz 4 VID die Frist beginnt, in der eine Verfügung über die Abweisung im Sinne von Artikel 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG; SR 172.021) verlangt werden kann (vgl. auch Erläuterungen zu Art. 27 Abs. 4 VID). Angesichts der Bedeutung für die gesuchstellenden Personen, rechtzeitig Kenntnis über eine Verweigerung zu erlangen, könnte eine systematische oder wiederholte Verletzung dieser Informationspflicht durch einen Registrar gar zur Auflösung des Vertrags führen, der ihn zur Ausübung seiner Tätigkeit berechtigt (vgl. Art. 17 Abs. 7 VID).

Art. 23 Abs. 3 Pflicht zur Zusammenarbeit

Aus Wirksamkeits- und Praktikabilitätsgründen muss der Prozess zur Bezeichnung einer Korrespondenzadresse in der Schweiz ("Rechtsdomizil") vereinfacht werden. Dazu wird der Prozessschritt, welcher die Registrare einbezieht, gestrichen. Die Registrare stehen folglich nicht mehr als Intermediäre zwischen Registerbetreiberin und Halterinnen oder Halter eines Domain-Namens (Streichung von Abs. 3 VID in Verbindung mit der Änderung von Art. 16 Abs. 3 VID; vgl. diesbezüglich auch die Erläuterungen zu Art. 16 Abs. 3 VID).

Art. 25 Abs. 3 Allgemeine Zuteilungsvoraussetzungen

Nach der bisherigen Regelung muss die Registerbetreiberin die Zuteilung eines Domain-Namens verweigern, wenn die Bezeichnung gegen die öffentliche Ordnung, die guten Sitten oder das anwendbare Recht verstösst oder technische Gründe dies erfordern (Art. 25 Abs. 2 VID). Ausserdem kann sie die Zuteilung verweigern, wenn die Gesuchstellerin oder der Gesuchsteller Konkurs anmeldet oder sich in Liquidation oder Nachlassstundung befindet (Abs. 3). Aufgrund der Erfahrungen der letzten Jahre und der Missbräuche, die insbesondere das SECO im Bereich E-Commerce festgestellt hat, erweisen sich die Möglichkeiten der Zuteilungsverweigerung als zu eingeschränkt. Gewisse bösgläubige Akteure zögern in der Tat nicht, die Neuzuteilung von Domain-Namen zu verlangen, für die gemäss Artikel 31 Absatz 3 VID noch eine Quarantänefrist läuft, nachdem beispielsweise ein Widerruf wegen Verletzung rechtlicher Bestimmungen wie jener zur Preisbekanntgabe stattgefunden hat.

Es ist neu vorzusehen, dass die Zuteilung von Domain-Namen verweigert werden muss, wenn berechtigte Gründe zur Annahme bestehen, dass die Gesuchstellerin oder der Gesuchsteller den beantragten Domain-Namen zu einem unrechtmässigen Zweck oder in unrechtmässiger Weise nutzen wird (Abs. 2 Bst. c). Eine solche Verweigerung ist jedoch vor dem Hintergrund zu betrachten, dass eine Registerbetreiberin lediglich eine technisch-administrative Schnittstelle ist, deren einzige Rolle darin besteht, den Nutzenden eine Ressource – d. h. die Domain-Namen – zur Nutzung des Internets zur Verfügung zu stellen. Weiter ist zu beachten, dass sie weder die Aufgabe noch die Kompetenz hat, die Rechtmässigkeit der Verwendung zugeteilter Domain-Namen zu beurteilen (vgl. Art. 10 Abs. 2 VID). Die Verweigerungspflicht für die Registerbetreiberin drängt sich deshalb nur dann auf, wenn sie rechtzeitig von einer im Rahmen ihrer Zuständigkeit intervenierenden Behörde ausführliche Hinweise zu einem bestimmten Domain-Namen erhält, der von einem Akteur beantragt werden könnte, welcher unrechtmässig oder zu einem unrechtmässigen Zweck handelt.

Eine Verweigerung muss ausserdem für Fälle vorgesehen werden, in denen die Gesuchstellerin oder der Gesuchsteller die Zuteilung desselben Domain-Namens beantragt, der gemäss Artikel 16 Ab-

satz 3 oder Artikel 15c Absatz 2 VID widerrufen worden ist, ohne eine gültige Korrespondenzadresse in der Schweiz zu bezeichnen (Bst. d).

Art. 27 Abs. 4 Zuteilungsverfahren

Die Registerbetreiberin behandelt ein Gesuch zur Registrierung eines Domain-Namens a priori nur mithilfe des den Registraren bereitgestellten elektronischen Registrierungssystems (Art. 10 Abs. 1 Bst. b, 24 Abs. 1 und 2, 27 Abs. 1–3 VID). Die Registrare fungieren so als exklusive Schnittstelle zwischen der Registerbetreiberin und der gesuchstellenden Person (Art. 24 Abs. 1 und Bst. m Anhang VID). Mit der vorgeschlagenen Ergänzung in Artikel 27 Absatz 4 VID ("... nachdem die Registerbetreiberin dem Registrar, der im Auftrag der betroffenen Gesuchstellerin oder des betroffenen Gesuchstellers tätig ist, die Verweigerung der Zuteilung mitgeteilt hat, ...") sowie der redaktionellen Anpassungen in der deutschen Version soll klargestellt werden, dass jede Zuteilungsverweigerung grundsätzlich nur über das Registrierungssystem und nur ausnahmsweise auf einem anderen Weg gemäss Absatz 3 kommuniziert wird. Ausserdem soll verdeutlicht werden, dass ab dieser Mitteilung, die die Registerbetreiberin dem im Auftrag der gesuchstellenden Person handelnden Registrar elektronisch übermittelt, die Frist beginnt, in der die gesuchstellende Person einen formellen Entscheid (eine Verfügung) verlangen kann. Der betroffene Registrar empfängt die elektronische Mitteilung über die Zuteilungsverweigerung umgehend, ohne zeitliche Verzögerung und ohne Anfechtungsmöglichkeit über das elektronische Registrierungssystem.

Die Frist von 30 Tagen, während der die von der Zuteilungsverweigerung betroffenen Gesuchstellerinnen und Gesuchsteller beim BAKOM einen formellen Entscheid im Sinne von Artikel 5 VwVG verlangen können, entspricht der ordentlichen Widerspruchs-, Einsprache- und Beschwerdefrist in Verwaltungsverfahren. Diese Frist wird vorliegend auf 40 Tage verlängert, um dem Umstand Rechnung zu tragen, dass sie ab der elektronischen Mitteilung der Zuteilungsverweigerung an den Registrar zu laufen beginnt, obwohl die gesuchstellende Person diese Information zu diesem Zeitpunkt möglicherweise noch nicht von ihrem Registrar erhalten hat (auch wenn ihr diese Information unverzüglich oder spätestens innerhalb von drei Tagen nach Mitteilung des Verweigerungsentscheids über das Registrierungssystem weiterübermittelt werden müsste [vgl. Erläuterungen zu Art. 21 Abs. 3 VID]). Durch die Verlängerung der Frist für das Verlangen eines formellen Entscheids auf 40 Tage wird berücksichtigt, dass die gesuchstellende Person zur Kenntnisnahme der Zuteilungsverweigerung hauptsächlich von der Sorgfalt ihres Registrars abhängig ist.

Art. 30 Abs. 3 Widerruf

Die provisorischen Massnahmen sind wichtig für das DNS, da die erfolgreiche Bekämpfung der Cyberkriminalität hauptsächlich davon abhängt, wie schnell einer Unregelmässigkeit oder einer Bedrohung begegnet werden kann. Die in Artikel 30 Absatz 3 VID vorgesehenen provisorischen Massnahmen müssen leicht angepasst und ergänzt werden:

- Die staatlichen Gerichte oder Schiedsgerichte, die staatlichen Behörden und andere Streitbelegungsdienste sind nicht mehr nur befugt, den Widerruf eines Domain-Namens gemäss Absatz 2, sondern neu auch provisorische Massnahmen anzuordnen. Deshalb muss der Wortlaut von Absatz 3 entsprechend angepasst werden. Die Registerbetreiberin führt die von diesen Organen geforderten Massnahmen aus, da sie a priori für die Umsetzung zuständig ist, auch wenn formell noch keine Verfügung erlassen worden ist. Wenn eine Massnahme aus Absatz 3 von einem dieser Organe provisorisch angeordnet wird, muss die Registerbetreiberin diese konsequent umsetzen respektive muss die Massnahme durch Expertenentscheide und Verfügungen von Behörden gemäss Artikel 5 VwVG, Schiedsentscheide oder andere Anordnungen, Gerichtsurteile und -entscheide bestätigt werden.
- Obwohl die Registerbetreiberin vor allem ein technisch-administrativer Akteur ist, der die Rechtmässigkeit der Nutzung von zugeteilten Domain-Namen nicht zu beurteilen hat (vgl.

- Art. 10 Abs. 2 VID), soll sie trotzdem die Kompetenz erhalten, selbst provisorische Massnahmen im Sinne von Absatz 3 zu ergreifen. Dies in zwei besonderen Fällen (Abs. 4):
- Wenn sich dies zum Schutz der Integrität und Stabilität des DNS als notwendig erweist und zeitliche Dringlichkeit besteht, einen drohenden, nicht leicht wiedergutzumachenden Nachteil abzuwenden (Bst. a). Das Ergreifen der geeigneten Massnahmen zur Sicherstellung der Zuverlässigkeit, Stabilität, Zugänglichkeit, Verfügbarkeit und Sicherheit der Infrastruktur sowie der für die Verwaltung des DNS notwendigen Dienstleistungen bildet eine der Hauptaufgaben einer Registerbetreiberin (vgl. Art. 10 Abs. 1 Bst. g VID).
 - Für höchstens fünf Werktage, wenn die Registerbetreiberin den begründeten Verdacht hat, dass die Halterin oder der Halter den Domain-Namen in unrechtmässiger Weise oder zu einem unrechtmässigen Zweck benutzt, und die zeitliche Dringlichkeit besteht, einen drohenden, nicht leicht wiedergutzumachenden Nachteil abzuwenden (Bst. b). Diese Bestimmung übernimmt die Regelung von Artikel 24h der Verordnung über die Adressierungselemente im Fernmeldebereich (AEFV; SR 784.104), die den Fernmeldediensteanbieterinnen ein provisorisches Sperren von einzeln zugeteilten Nummern ermöglicht. Vorliegend wird die Sperrfrist im Einklang mit Artikel 15 Absatz 1 VID auf fünf Werktage ausgedehnt.
- Der Katalog an provisorischen Massnahmen in Absatz 3 muss präzisiert und ergänzt werden, wodurch alle Unsicherheiten bezüglich der Massnahmen, die tatsächlich ergriffen werden können, beseitigt werden können und die sich auf internationaler Ebene entwickelnde Praxis berücksichtigt werden kann (vgl. insbesondere ICANN, Framework for Registry Operator to Respond to Security Threats):
- Gemäss Buchstabe a kann die Registerbetreiberin auf alle möglichen Arten auf Ebene der Namensserver ("Domain Name Server") handeln, die mit bestimmten Domain-Namen verbunden sind. Die Namensserver weisen einem Domain-Namen eine IP-Adresse im Internet zu (Auflösung) und sichern so deren Verbindung zum Internet. Die Registerbetreiberin kann künftig die mit einem Domain-Namen verbundenen Namensserver in der Zonendatei provisorisch löschen und somit den betroffenen Domain-Namen sperren oder zwecks Umleitung des Datenverkehrs die Namensserver mit neuen ersetzen (vgl. Bst. g). Des Weiteren muss sie die zuvor aus der Zonendatei gelöschten Server nicht zwingend wieder einfügen, sodass die Halterinnen und Halter der Namen selber dafür sorgen müssen (vgl. diesbezüglich auch die Erläuterungen zu Art. 15 VID).
 - Buchstabe b erlaubt es künftig unter dem Titel der administrativen Sperrung nicht nur, die Neuzuteilung eines einer Halterin oder einem Halter gehörenden Domain-Namens, sondern auch die Zuteilung eines freien Domain-Namens an einen Dritten zu verhindern. Ausserdem sollen diejenigen automatisch durch DGAs generierten Domain-Namen, die frühzeitig erkennbar sind, gesperrt werden (cf. Erläuterungen zu Art. 15 und 15a VID).
 - Gestützt auf Buchstabe c kann von der Registerbetreiberin verlangt werden, dass die administrative Verwaltung eines Domain-Namens an einen anderen Registrar übertragen wird (vgl. Bst. t Anhang VID). Dadurch kann böswillig handelnden Registraren entgegengewirkt werden, die sich an illegalen Handlungen ihrer Kundinnen und Kunden (Nutzer/innen von Domain-Namen) beteiligen, solche fördern oder decken.
 - Die Buchstaben d und e erlauben jegliche Änderung, Korrektur oder Löschung von Informationen oder technischen oder administrativen Parametern, welche die Verwaltung eines Domain-Namens betreffen (z. B. technischer Kontakt [Tech-C], administrativer Kontakt [Admin-C]) oder jene in der WHOIS-Datenbank (cf. Art. 46, 52 und Bst. k Anhang VID).
 - Buchstabe f ermöglicht es der Registerbetreiberin, einen Domain-Namen sich selber oder einer Person zuzuteilen, die von der zuständigen, diese Massnahme anordnenden Stelle bezeichnet wird.
 - Neben den in den Artikeln 15 ff. VID vorgesehenen Verfahren und Kompetenzen kann auch Sinkholing provisorisch angeordnet werden. Diese Massnahme muss von der

Registerbetreiberin auf Ersuchen einer zuständigen Behörde ergriffen werden (Bst. g; vgl. diesbezüglich auch die Erläuterungen zu Art. 15a und 15d VID).

Schliesslich ist darauf hinzuweisen, dass die Terminologie in Absatz 3 in der deutschen Version angepasst wurde, um sie jener anderer Erlasse anzugleichen ("sperrern" anstatt "blockieren").

Art. 46 Abs. 1 Bst. b–f Öffentlich zugängliche Daten

Gemäss Artikel 46 Absatz 1 Buchstabe e VID muss die massgebende Sprache für die Durchführung eines allfälligen Streitbeilegungsverfahrens im Sinne von Artikel 14 VID in der WHOIS-Datenbank veröffentlicht werden (Bst. k Anhang VID). Eine solche Veröffentlichung wäre mit tiefgreifenden Änderungen im WHOIS-Informatiksystem und einem grossen Verwaltungsaufwand verbunden. Es müssten die entsprechenden Informationen für alle rund zwei Millionen bisher zugeteilten .ch-Domain-Namen eingeholt werden. Dieser Aufwand erscheint unverhältnismässig, da die massgebende Sprache nur in einigen wenigen Fällen pro Jahr bekannt sein muss und die Information auf Ersuchen der Registerbetreiberin für jeden Streitfall einzeln geliefert werden kann, ohne dass dies Auswirkungen auf das Streitbeilegungsverfahren hätte. Buchstabe e wird folglich aufgehoben.

Darüber hinaus muss der Buchstabe d aufgehoben werden, in dem die Veröffentlichung des Namens einer natürlichen Person, die mit der Vertretung der betroffenen juristischen Person betraut ist, verlangt wird. Diese Verpflichtung ist für die juristischen Personen oder deren Registrare nicht klar, da diese oft interne Stellen angeben ("Domain-Namen-Administrator", "Informatikdienst", "Hostmaster" oder "Kundendienst"). Zudem schafft die Angabe einer einzigen natürlichen Person letztlich nicht wirklich Klarheit über die rechtliche Vertretung einer juristischen Person. Für die rechtsgültige Vertretung einer juristischen Person ist oft die Zustimmung von zwei Personen erforderlich (Kollektivunterschrift zu zweien). Die Zeichnungsberechtigungen und die entsprechenden Handelsregistereinträge können jederzeit ändern.

Schliesslich können die Buchstaben b und c (Angaben zur Halterschaft) sowie f (Angaben zu den technisch verantwortlichen Personen) wie für die Domain .swiss in Artikel 52 Absatz 1 VID vereinfacht werden. Insbesondere kann die überflüssige Angabe des Staates oder der Provinz gestrichen werden. Hingegen müssen die zwingend in der WHOIS-Datenbank abrufbaren Angaben mit den Daten zu den Namensservern, die einem Domain-Namen bei einer Aktivierung zugewiesen werden (neuer Bst. c), ergänzt werden. Bei dieser Gelegenheit soll auch der Wortlaut von Artikel 52 Absatz 1 Buchstabe e VID für .swiss präzisiert werden ("bei einem aktivierten Domain-Namen"), da ein Domain-Name auch zugeteilt werden kann, ohne dass ihm zwingend Namensserver zugewiesen sind (in der Praxis werden zwei Namensserver pro aktivierten Domain-Namen benötigt).

Art. 52 Abs. 1 Bst. e Öffentlich zugängliche Daten

Mit Ausnahme der mit Namenszuteilungsmandat zugeteilten Domain-Namen (Art. 56 Abs. 7 VID) muss ein .swiss-Domain-Name nicht zwingend aktiviert werden, d. h. ihm müssen keine Namensserver zugewiesen werden, die die Verbindung zum Internet ermöglichen würden. Nur bei einer Aktivierung müssen die mindestens zwei einem bestimmten Domain-Namen zugeteilten Namensserver in der WHOIS-Datenbank aufgeführt werden (Abs. 1 Bst. e).

Art. 54 Privilegierte Zuteilung

In Artikel 54 VID wird die Phase der privilegierten Zuteilung von .swiss-Domain-Namen geregelt ("sunrise period"), die der allgemeinen Öffnung der Domain .swiss am 11. Januar 2016 vorausgegangen ist. Da sich die Domain nun im ordentlichen Betrieb befindet, sind die Spezialregeln von Artikel 54 VID hinfällig und müssen folglich aufgehoben werden.

Art. 55 Berechtigung

Der bisherige Artikel 55 VID ermöglicht die gestaffelte Öffnung der Berechtigung für die Zuteilung eines .swiss-Domain-Namens in Abhängigkeit der verschiedenen Kategorien von zuteilungsberechtigten Personen. Dabei wird dem UVEK die Planung übertragen. Das Departement hat seine Aufgabe

durch den Erlass der Verordnung vom 11. August 2015 über die Internet-Domain .swiss (SR 784.104.253) erfüllt. In dieser wird bis zum 31. Dezember 2017 die Berechtigung für natürliche Personen mit Wohnsitz in der Schweiz oder Schweizer Bürgerrecht ausgeschlossen.

Die Berechtigung neu auf natürliche Personen auszudehnen ist zurzeit weder beabsichtigt noch wünschenswert. Wie der Bundesrat mehrfach betont hat, zielt die Verwaltung von .swiss durch den Bund vor allem darauf ab, die Interessen der Schweiz zu wahren, indem die neue Internet-Domain .swiss der Wirtschaft, Kultur und den Institutionen des Landes zur Verfügung gestellt wird. Die Domain .swiss ist demnach zum Schaufenster der Schweizer Unternehmen und Institutionen geworden, die von einer klaren Herkunftsangabe im Internet profitieren können. Diese Positionierung beruht auf Vorabklärungen bei interessierten Kreisen, wurde von Marketingkampagnen gefördert und hat sich in den Wirtschaftskreisen durchgesetzt sowie in den Köpfen der Schweizerinnen und Schweizer eingepreßt. Die Domain .swiss wird deshalb künftig als Ergänzung zur sehr beliebten .ch-Domain angesehen. Während jede natürliche Person die Zuteilung eines .ch-Domain-Namens beantragen kann, können sie dies bei .swiss nur als im Handelsregister eingetragene Einzelunternehmen (Bst. b). Die Öffnung von .swiss für natürliche, nicht als Einzelunternehmen im Handelsregister eingetragene Personen ist zum jetzigen Zeitpunkt kaum gerechtfertigt. Im Gegenteil: Eine solche Öffnung könnte dem nationalen und internationalen Image von .swiss sowie der aktuellen Positionierung schaden. Ausserdem würde dies bei den Schweizer Unternehmen, die bereits in .swiss investiert haben, angesichts der legitimen Erwartungen, die diese Unternehmen gegenüber der Domain entwickelt haben, auf Unverständnis stossen. Schliesslich könnte eine Öffnung derzeit dazu führen, dass die Marktposition der beiden Domains .ch und .swiss geschwächt würde.

Angesichts der Tragweite und der weitreichenden Konsequenzen eines solchen Entscheids muss dem Bundesrat die Kompetenz übertragen werden festzulegen, ob und wann eine allfällige Öffnung der Berechtigung für die Zuteilung von .swiss-Domain-Namen zugunsten von natürlichen Personen dank einer Änderung der Liste der zugangsberechtigten Personen in Artikel 55 VID stattfinden könnte. Die derzeitige Delegation der Zuständigkeit an das UVEK wird künftig gestrichen und dessen Verordnung über die Internet-Domain .swiss aufgehoben (siehe oben).

Art. 61–64 Übergangsbestimmungen

Die Übergangsbestimmungen äussern sich zu den Rechten und Pflichten von SWITCH im Rahmen des Delegationsverhältnisses nach dem Vertrag vom 31. Januar 2007. Die Bestimmungen sind obsolet geworden und können demzufolge aufgehoben werden.

Anhang

Die Definition von "Bezeichnung mit generischem Charakter" im Anhang der VID (Bst. q) wird leicht abgeändert. In der Aufzählung der Kategorie oder Gattung von allem, das eine Bezeichnung mit generischem Charakter im Sinne der VID darstellt, wird der Begriff "Dinge" durch "Produkte" ersetzt.

Der Begriff "Dinge" bezieht sich auf alles, was ist und existiert, auf die Realität jeglicher Art. Dieser Oberbegriff hat sich letztlich als zu breit erwiesen, da er Bezeichnungen umfasst, die nicht unter Artikel 56 VID fallen sollen. Letzterer zielt hauptsächlich darauf ab, jene Bezeichnungen zu schützen, die als Domain-Namen den jeweiligen Halterinnen und Haltern einen unverhältnismässigen Wettbewerbsvorteil im Internet gewähren würden und deren Monopolisierung dem Interesse der Schweizer Gemeinschaft zuwiderläuft. Der Begriff "Produkte", der für Dinge, Substanzen und andere Güter steht, die von Menschen hergestellt und allgemein vermarktet sind, ist besser geeignet, um das Ziel zu erreichen, das mit den Bestimmungen der VID betreffend die Bezeichnungen mit generischem Charakter verfolgt wird.

Aufhebung

Die Verordnung des UVEK vom 11. August 2015 über die Internet-Domain .swiss (SR 784.104.253) hat keine eigenständige Bedeutung mehr und muss deshalb aufgehoben werden:

- Die auf Grundlage von Artikel 54 VID angebrachten Präzisierungen zur Phase der privilegierten Zuteilung von .swiss-Domain-Namen ("sunrise period") sind hinfällig, da die Domain .swiss sich nun im ordentlichen Betrieb befindet.
- Die Frage nach der gestaffelten Öffnung der Berechtigung an der Zuteilung eines .swiss-Domain-Namens wird künftig ausschliesslich in Artikel 55 VID geregelt (vgl. oben Erläuterungen zu Art. 55 VID).