2/2016
25 – 48

DSGVO
„One Stop Shop"-Prinzip
G. Leissler, V. Wolfbauer

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Cybercrime

Praxisfall Cyberangriff – hätten Sie ihn erkannt?
Lars D. Preußer

Die Täter sind professioneller geworden
Interview mit Leopold Löschl

Cyber-Versicherung
Thomas Hubinger

Datenmissbrauch: Ernstfall und Vorbereitung
Rainer Knyrim, Clemens Foisner, Paul Prihoda

In Cybercrime verfangene Domains „einfangen"
Rainer Knyrim, Boris Treml

Checkliste Datensicherheitsmaßnahmen
Hans-Jürgen Pollirer

Mit Standardvertragsklauseln in die Cloud
Rainer Knyrim

Gesetzesbeschwerde
Ernst M. Weiss

ISSN 2313-5409

dako.manz.at

MANZ

P.b.b. Verlag Manz 1230 Wien, Gutheil Schoder Gasse 17

Rainer Knyrim/Boris Treml
Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte/ Rechtsanwaltsanwärter bei Preslmayr Rechtsanwälte

In Cybercrime verfangene Domains „einfangen“

Identitätsdiebstahl, Schlichtungsverfahren, WIPO. Cybercrime-Angriffe gehen häufig mit einem Identitätsdiebstahl einher. Mit dem Verfahren nach der Uniform Domain Name Dispute Resolution Policy (UDRP) der Internet Corporation for Assigned Names and Numbers (ICANN) kann die digitale Identität wieder „eingefangen“ werden.

Opfer von Cybercrime-Angriffen sehen sich oft mit einem Identitätsdiebstahl konfrontiert. Dabei registriert der Angreifer die vom Opfer registrierte Domain in einer ähnlichen Variante.

BEISPIELE

wikkipedia.com[1], raiffeien.ch[2], blackbberry.com[3] oder hoildayinnexpress.com[4]; bei diesen Domains wurde die Technik des Typosquatting angewandt. Dabei wird durch geschicktes Hinzufügen oder Weglassen von Buchstaben ein fast identer Domain-Name geschaffen:[5] das zweite „k“ bei wikkipedia.com, das fehlende „s“ bei raiffeien.ch, ein „b“ zu viel bei blackbberry.com oder die verdrehte „il“-Kombination bei hoildayinnexpress.com.

Solche Domains werden von Betrügern verwendet, um damit E-Mail-Adressen zu bilden, die zB jener des Geschäftsführers oder Finanzchefs eines Unternehmens zum Verwechseln ähnlich sehen (zB vorname.nachname@hoildayinnexpress.com), und mit der sich die Betrüger in einem Cyber-Angriff in die Unternehmenskommunikation „einmischen“, um zB falsche Zahlungsanweisungen zu geben. Den Verlauf eines solchen Angriffs beschreibt *Preußer* in seinem Beitrag in diesem Heft Seite 28.

Handeln bei Kenntnisnahme der Cyber-Attacke

Entdeckt das Opfer, dass ein Dritter eine ähnliche Domain für Cyber-Angriffe nutzt oder nutzen will, ist der **Registrar**, also jene Stelle, die die Domain vergeben hat, über die unrechtmäßige Nutzung in Kenntnis zu setzen. Die Kenntnisnahme durch den Registrar führt nämlich zum Entfall der Haftungsbefreiung iSd E-Commerce-Gesetzes und der Registrar wird durch die Setzung des Status „clientHold“ für die betreffende Domain dafür sorgen, dass diese nicht weiter verwendbar ist.

Einfangen der Domains

Wer auf Nummer sicher gehen will, dass die in den Cyber-Angriff verfangene Domain nicht für einen erneuten Angriff nutzbar ist (etwa durch eine erneute Registrierung der Domain bei einem anderen Registrar nach Ablauf der Registrierungsperiode), muss dafür Sorge tragen, dass die Domain auf ihn übertragen wird. Dafür ist es not-

[1] Verfahren Nr D2015–1404. [2] Verfahren Nr DCH2012–0024.
[3] Verfahren Nr D2009–0322. [4] Verfahren Nr D2003–0663.
[5] https://de.wikipedia.org/wiki/Typosquatting

wendig, den **Aufbau einer Domain** zu **prüfen**. Die Prüfung erfolgt von rechts nach links, wobei die Bestandteile der Domain durch einen Punkt getrennt sind. Der ganz rechts stehende Name wird als Top-Level-Domain bezeichnet. Dieser folgt die Second-Level-Domain, dieser die Third-Level-Domain.

Um zu bestimmen, welche Verfahren für eine Übertragung der Domain in Frage kommen, ist eine Auseinandersetzung mit der **Top-Level-Domain** geboten.[6] Die Top-Level-Domain kann in zwei Gruppen geteilt werden,

- in die der Country code Top-Level-Domain (ccTLD), das sind zum Beispiel Domains, die auf .de, .at. oder .uk enden, und
- in die Generic Top-Level-Domains (gTLD), das sind Domains, die beispielsweise auf .com, .org oder .net enden.

Sowohl die ccTLD als auch die gTLD werden von der Internet Assigned Numbers Authority (IANA), einer Abteilung der Internet Corporation for Assigned Names and Numbers (ICANN), verwaltet.

Die ICANN hat im Jahr 1999 die **Uniform Domain Name Dispute Resolution Policy** (UDRP) veröffentlicht. Es handelt sich hierbei um ein Regelwerk für ein Schlichtungsverfahren, das vor der WIPO, NAF oder CAC[7] geführt werden kann. Voraussetzung für die Anwendbarkeit der UDRP ist, dass sich der Registrar diesem Verfahren unterworfen hat und dieses auch auf den jeweiligen Registrant überbindet. Dies ist obligatorisch für alle gTLD und fakultativ bei den ccTLD. Wird eine Cyber-Attacke unter Verwendung einer ccTLD, das ist bspw eine .at-, .de- oder .fr-Domain, verwirklicht, muss geprüft werden, ob der Registrar die UDRP für anwendbar erklärt hat. Dies ist bspw bei .at-Domains nicht der Fall, weshalb das Schlichtungsverfahren nicht anwendbar ist. Der Registrant hat somit den Zivilrechtsweg zu beschreiten, wobei zu berücksichtigen ist, dass ein Anspruch auf Übertragung von Domains in stRsp abgelehnt wird.[8] Bei .at-Domains, die vom Registrar nic.at GmbH verwaltet werden, können uU deren AGB[9] ein Einfangen der verfangenen Domain ermöglichen. In Abschnitt 1.3 ist vorgesehen, dass der Domain-Inhaber eine ladungsfähige physische Adresse bei der Registrierung angeben muss. Sollte diese nicht vorhanden sein – was bei Betrügern der Fall sein wird –, hat sich die nic.at GmbH das Recht vorbehalten, die Registrierung zu widerrufen oder abzulehnen. Widerruft nun nic.at GmbH die Registrierung aus diesem Grund, könnte die .at-Domain im nächsten Schritt vom Opfer selbst registriert werden, womit die streitverfangene Domain eingefangen ist.

Einfaches Schlichtungsverfahren der WIPO

Vergleichsweise einfach scheint hier das UDRP-Verfahren. Dieses Verfahren wird wie folgt abgewickelt: Nachdem die Prüfung über die Anwendbarkeit der UDRP bejaht worden ist, ist ein Antrag nach Maßgabe der UDRP zu verfassen und bei der gewählten Schlichtungsstelle einzubringen.

Der Antrag muss ua Folgendes thematisieren:

- Die verfangene Domain verletzt Markenrechte des Beschwerdeführers oder es besteht Täuschungsgefahr,
- kein eigenes Recht oder berechtigtes Interesse des Beschwerdegegners an der verfangenen Domain und
- die bösgläubige Registrierung und Benutzung des Domainnamens.

Die Sprache, in der der Antrag zu verfassen ist, richtet sich nach der Vertragssprache der Registrierung der entsprechenden Domain. Die Verfahrenskosten belaufen sich auf USD 1.500,–, wenn das Erkenntnis des Schiedsgerichts von einem Einzelschiedsrichter getroffen wird. Mehrere Domains können in einem Verfahren gebündelt werden, wenn diese bei demselben Registrar registriert wurden. Die Schiedsstelle prüft und verständigt die Verfahrensparteien über den Antrag und bietet die Möglichkeit der Stellungnahme. Im nächsten Schritt ist der erkennende Schiedsrichter zu bestellen. Gibt dieser dem Antrag statt, hat der Registrar die Domain an den Registrant zu übertragen.

PRAXISTIPP

Die WIPO hat auf ihrer Homepage ein Ausfüllmuster zur Verfügung gestellt und publiziert sämtliche Entscheidungen ebendort.

Fazit

Das anhand der UDRP geführte Übertragungsverfahren vor der WIPO ist als erprobt und praxistauglich für Domainübertragungen zu bezeichnen.[10] Die Vorteile liegen auf der Hand: Der Zeit- und Kostenaufwand ist für den Beschwerdeführer überschaubar, da das Verfahren als reines Aktenverfahren konzipiert ist und die Verfahrenskosten pauschal verrechnet werden.

PRAXISTIPP

Wer im Verfahren mit Markenrechten argumentieren kann, ist klar im Vorteil. Aus rein praktischen Überlegungen empfiehlt es sich, die Domains, die zur Kommunikation nach außen verwendet werden, möglichst gering zu halten, weil jede neue Domain weitere Angriffspunkte darstellt. Empfehlenswert scheint auch die Prüfung, ob Domains registriert wurden, die mit der eigenen Domain Verwechslungpotential aufweisen.[11]

Dako 2016/21

[6] https://de.wikipedia.org/wiki/Top-Level-Domain [7] World Intellectual Property Organization, National Arbitration Forum, Czech Arbitration Court. [8] OGH 4 Ob 226/04w; 4 Ob 59/13z; 4 Ob 75/15f. [9] www.nic.at/fileadmin/www.nic.at/documents/rechtliches/AGB-2015.pdf [10] Die Autoren haben nach einem Cyberangriff auf ein österreichisches Unternehmen fünf WIPO-Übertragungsverfahren zu Typosquatting-Domains erfolgreich durchgeführt, die allesamt rasch und erfolgreich abliefen. [11] www.trademarks.thomsonreuters.com/de/recherche/web-recherchen?cid=179&id=produkt%2Fdomain-typo-squatting-search

Zum Thema

Über die Autoren

Dr. Rainer Knyrim ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte in Wien.
Tel: +43 (0)1 533 16 95, E-Mail: knyrim@preslmayr.at, Internet: www.preslmayr.at
Ing. Mag. Boris Treml LL.M ist Rechtsanwaltsanwärter bei Preslmayr Rechtsanwälte in Wien.
Tel: +43 (0)1 533 16 95, E-Mail: treml@preslmayr.at, Internet: www.preslmayr.at

Linktipp

- Ausfüllmuster der Wipo: www.wipo.int/amc/en/domains/complainant/
- Entscheidungen der Wipo: www.wipo.int/amc/en/domains/search/fulltext_decisions.jsp