

# Newsletter April 2021



- **Brand bei europäischem Cloudanbieter** ✓
- **Kriminelle mit schlechtem Gewissen** ✓
- **Sicherheit im Wandel der Zeit** ✓
- **Neues von den Domains: .gov, .is, .uk, .watches und .xxx** ✓

## Brand bei europäischem Cloudanbieter

Das Straßburger Rechenzentrum eines großen europäischen Cloudanbieters wurde am 10. März Opfer eines Brandes. Über 100 Feuerwehrleute kämpften ab Mitternacht bis in die Morgenstunden gegen die Flammen. Auch wenn glücklicherweise keine Menschen verletzt wurden, werden die Auswirkungen noch eine ganze Weile zu spüren sein. Einer der vier Blöcke des Rechenzentrums wurde komplett vernichtet, ein anderer schwer beschädigt. In allen vieren wurde während des Brandes der Strom abgeschaltet. Die Wiederherstellung der Dienste dauert noch an.

Der wirtschaftliche Schaden ist gigantisch. Über 3,5 Millionen Webseiten sind teilweise bis jetzt nicht mehr erreichbar. Die schlimmste Nachricht ist aber: Für die meisten Kunden wurden auch die Datensicherungen, die im jeweils gleichen Block verortet waren, vernichtet. Wenn sie überhaupt vorhanden waren - ein dezentrales Backup war nicht vorgesehen. Sofern die Kunden nicht für eine eigene Sicherungsstrategie gesorgt hatten, stehen sie mit leeren Händen da.

Der Vorfall bedeutet auch ein Rückschlag für die europäische Cloudinitiative GAIA-X. Diese will ein Gegengewicht zu den hauptsächlich amerikanischen Cloudanbietern setzen und hatte dabei auch Ressourcen aus Straßburg eingeplant. Die Initiatoren müssen nun erstmal ihre Standards überdenken. Leider wird oft erst im Schadenfall deutlich, wie wichtig ein durchdachtes Sicherheitskonzept ist. Wie Sie Ihre Daten dezentral schützen können, erläutert Ihnen unser Vertrieb.

## Kriminelle mit schlechtem Gewissen

Auch das gibt es: Die Macher des Verschlüsselungstrojaners Ziggy haben mitgeteilt, dass sie aus moralischen Gründen und aus Angst vor der Strafverfolgung ihre Aktion rückgängig machen. Als ersten Schritt veröffentlichten sie ein kostenloses Entschlüsselungstool, mit dem die Daten der betroffenen Rechner wieder nutzbar werden. Wer auf die Lösegeldforderung der Ex-Erpresser bereits eingegangen ist, möge sich per Mail an den ‚Support‘ von Ziggy wenden und erhalte innerhalb von zwei Wochen sein Geld zurück.

Ein solches Entgegenkommen würden sich Opfer des nach wie vor gefährlichsten Trojaners Emotet auch wünschen. Zwar gelang es IT-Ermittlern jüngst in einer groß angelegten, internationalen Aktion, die zugehörige Serverinfrastruktur lahmzulegen und einige der Beteiligten zu verhaften. Es steht aber zu befürchten, dass dies nur ein Rückschlag für Emotet sein wird, nicht aber das Ende.

## Sicherheit im Wandel des Zeit

Ohne Verschlüsselung ist das heutige Internet undenkbar. Das wichtigste Verfahren ist TLS (Transport Layer Security), das unter anderem die Verbindung zwischen Webserver und Webbrowser schützt. TLS wird auch heute noch als SSL (Secure Socket Layer) bezeichnet, obwohl es sich technisch gesehen um den Nachfolger handelt. Das erklärt sich dadurch, dass Webserver lange Zeit SSL und TLS parallel angeboten haben und der Webbrowser des Besuchers sich die beste Verschlüsselung aussuchte, die er verarbeiten konnte. Dadurch überlebte der Name SSL. Der Standard SSL ist aber auch in seiner neuesten Version 3.0 seit 2015 veraltet. In diesem Jahr sorgte die nicht zu behebbende Sicherheitslücke „Poodle“ für sein Ende.

Aber auch beim Nachfolger TLS stehen die Uhren nicht still. Im März erklärte die Internet-Standardisierungsorganisation IETF die Versionen TLS 1.0 und 1.1 für veraltet. Die Nachfolger TLS 1.2 und höher können weiter eingesetzt werden.

Administratoren sollten jetzt ihren Gerätepark auf TLS 1.0 überprüfen. Während TLS 1.1 nie einen Durchbruch erlebt hat, findet sich TLS 1.0 vor allem noch bei ‚Appliances‘ wie Firewalls oder Virenschannern.

## Neues von den Domains

.gov

Die für die U.S.-Regierung gedachte Endung .gov wird zukünftig von Cybersecurity and Infrastructure Security Agency verwaltet. Die CISA ist mit dem deutschen BSI vergleichbar.

ICM

Schon lange bietet ICM für .adult, .porn, .sex und .xxx Defensivregistrierungen an, die zu einem vergünstigten Preis den Schutz von Markenrechten in den TLDs beinhaltet. Dieser Schutz wird nun deutlich erweitert. Der AdultBlock+ genannte Dienst blockt nun auch Varianten des Markennamens, z.B. meine-marke.xxx und meinemarke.xxx. Bei Interesse wenden Sie sich bitte an unseren Support.

.is

Nach mehreren Preissenkungen erhöhen sich zum ersten Mal die Kosten für .is-Domains. Dies sei auf gestiegene Löhne in Island zurückzuführen, die nicht mehr durch technische Weiterentwicklungen aufgefangen werden konnten.

.uk

Entgegen unserer Erwartung wurde das Direktorium von Nominet mit einer knappen Mehrheit von 53% zu 47% der Stimmen abgewählt. Nominet verwendet ein gewichtetes Wahlsystem, Registrare mit vielen Domains haben entsprechend mehr Stimmen. Den Verfechtern der Abwahl war es gelungen, einige der großen Registrare von der eigenen Meinung zu überzeugen. Diese störten sich vor allem an den hohen Vergütungen des Direktoriums. Der Geschäftsführer der Organisation hatte bereits am Vortag der Wahl seinen Rücktritt erklärt.

Es wurde ein Interimsvorstand berufen, der die Herstellung von Stabilität als seine wichtigste Aufgabe bezeichnet. Der technische Betrieb läuft derweil wie gewohnt weiter.

.watches

Die primär für Luxusgüter gedachte .watches wechselt den Besitzer und gehört nun zum Donuts-Konsortium. Richemont (Cartier, Piaget) hat sich damit von der letzten seiner 14 TLDs verabschiedet.

Mit freundlichen Grüßen

Ihr Global Village Team