Newsletter August 2021

- **Sicherheit von Microsoft Exchange**
- **Russland sperrt ungenehme Webseiten**
- **Billige Bitcoins**
- **Neues von den Domains: .bank, .de, .eu, .hu, .tickets, Minds&Machines**

Sicherheit von Microsoft Exchange

Eine Reihe von Ländern und Verbünden, darunter die E.U. und die U.S.A., betrachten es als erwiesen, dass China gezielt Microsoft Exchange Server angreift um Geschäftsgeheimnisse zu stehlen. Der dabei entstandene Schaden liegt im Milliardenbereich, wobei hier auch Schäden durch Krypto-Erpressungstrojaner mit einfließen.
Durchgeführt worden seien die Attacken von den Hackergruppen APT31 und ATP40. Diese vermarkten ihre Dienste an das dortige Ministerium für Staatssicherheit.
Zugute kam der Gruppe dabei eine Sicherheitslücke, die bereits im Januar bekannt war, aber erst im März von Microsoft beseitigt wurde. Das war mehr als genug Zeit, um sich tief in die Netzwerke der Betroffenen einzugraben.
Das hiesige Bundesministerium für Sicherheit in der Informationstechnik hat im März die Bedrohungsstufe Rot ausgerufen und im April alle national erreichbaren Exchange Systeme gescannt. Falls diese die Sicherheitslücke noch aufwiesen, wurden deren Administratoren informiert. Trotz dieser Maßnahme sind bis heute tausende Exchange Server nicht abgesichert. Das wird zum Teil daran liegen, dass der Update Prozess von Exchange nicht immer trivial ist und teilweise von den Betreibern zurückgenommen wurde, um den Betrieb aufrecht zu erhalten. Das ist ein mehr als gewagtes Spiel, denn nach einem Einbruch ist der Schaden fast immer größer als wenn ‚nur' E-Mail und Teamfunktionen nicht mehr zur Verfügung stehen. Alle Betreiber von Exchange sollten daher dringend die Aktualität ihrer Serverdienste prüfen.

Russland sperrt ungenehme Webseiten

Die russische Regierung verschärft vor der Parlamentswahl im September die Gangart gegenüber kritischen Stimmen. Das jüngste Opfer sind 50 Webseiten von Kreml-Kritikern, darunter alle Webseiten des weiterhin inhaftierten Alexej Nawalny. Dessen spektakuläre Videos über eine mutmaßliche Putin-Villa im Milliardenwert und Enthüllungen über den Parlamentspräsidenten und Milliardär Wjatscheslaw Wolodin hatten im Land für großes Aufsehen gesorgt.
Es traf aber auch unliebsame Organisationen, die sich nicht direkt gegen die jetzige Regierungspartei Geeintes Russland um Stimmen bemühen. Die Unabhängige Allianz der Ärzte, die auf Missstände in der Coronapolitik des Landes hingewiesen hatte, ist ebenfalls von der Sperre betroffen.
Derzeit lassen sich die Maßnahmen noch mithilfe eines VPNs umgehen. Die breite Masse potenzieller Besucher wird solche Umwege aber nicht gehen wollen. Zukünftig ist damit zu rechnen, dass auch solche Ersatzlösungen nicht mehr möglich sind. Russland treibt ein Programm voran, dass es im Zweifel ermöglichen soll, den russischen Teil des Internets vom Rest der Welt abzukoppeln.

Billige Bitcoins

.. wollten eine Reihe von Malaysiern schürfen und damit das große Geld verdienen. Dazu zapften sie das öffentliche Stromnetz an, um damit Rechnerfarmen zu betreiben. Leider gingen sie dabei sowohl ohne Rücksicht auf Verluste als auch dilettantisch vor. Der hohe Stromverbrauch führte zu mehreren Stromausfällen, die zum Teil aufgrund von Kaskaden, größere Gebiete im Bezirk Miri betrafen. Schlimmer noch, mehrere Häuser gerieten durch unfachmännisch verlegte Leitungen in Brand.
Alleine 1,7 Millionen Euro Schaden seien durch den Stromklau entstanden. Die Staatsgewalt setzte daraufhin dem Treiben ein Ende und vernichtete über 1.000 der beteiligten Rechner. Warum die hochwertigen Systeme nicht verkauft und für legale Zwecke eingesetzt wurden, bleibt rätselhaft.

Neues von den Domains

.bank

Der Betreiber fTLD zieht die Zügel für Sicherheits-anforderungen von .bank-Domains an. Die für die Praxis wichtigste Änderung besagt, dass Webweiterleitungen nur noch per HTTPS erlaubt sind. Marktüblich ist, dass der Weiterleitungsserver HTTP-Verbindungen annimmt und nur das Weiterleitungsziel eine HTTPS-URL hat. Das ist unter den neuen Bedingungen nicht mehr erlaubt.

.de

Im Juli wurde mit der Domain melba-stoffkreation.de der 17 Millionste Name unter .de freigeschaltet. Damit besitzt rechnerisch jeder fünfte Deutsche eine .de-Domain. Zudem sind 1,5 Millionen .de-Domains mit ausländischen Inhabern bekannt. Das ist internationaler Spitzenplatz, sieht man von den knapp 25 Millionen .tk-Registrierungen ab, denen gerade einmal 1.500 Einwohner gegenüberstehen. .tk-Domains werden aber fast ausschließlich von Ausländern genutzt.

.eu

Der aktuelle Betreiber EURid bemüht sich um eine Verlängerung seines Vertrages zum Betrieb von .eu. Dieser sollte planmäßig am Jahresanfang auslaufen, wurde aber übergangsweise verlängert. EURid muss sich dabei in einem Ausschreibungsverfahren gegen drei Konkurrenten, unter anderem die Registry Estlands, durchsetzen. Alle Teilnehmer sind bedingungsgemäß non-Profit-Organisationen.

.hu

Die Mindestlaufzeit für ungarische Domains verkürzt sich von 2 Jahren auf 1 Jahr.

.tickets

Bislang waren .tickets-Domains nur für Interessenten aus dem Ticketgewerbe zugänglich. In Kürze öffnet sich die TLD für jedermann.

Minds & Machines

Der Kauf der Registry (unter anderem .nrw und .bayern) durch GoDaddy wurde vom Regulierer ICANN abgesegnet. Die TLDs werden in den nächsten Monaten vom bisherigen technischen Betreiber Nominet zum neuen Besitzer umziehen.

Mit freundlichen Grüßen,
Ihr Global Village Team