Newsletter August 2022

- **Microsoft Office bleibt unsicher**
- **Russland übernimmt Apple**
- **Neues von den Domains: .eu, .fr, .kids, .ua, .za, Centralnic**

Microsoft Office bleibt unsicher

Einfallstor Nummer 1 für Verschlüsselungstrojaner, Spionagesoftware und Viren sind immer noch Makros in Dokumenten von Microsoft Office. Den Schaden trägt aber nicht Microsoft, sondern die betroffenen Unternehmen. Die Hackergruppen sind dabei mittlerweile professionell genug, herauszufinden, welche Schmerzgrenze ihre Opfer besitzen und ihre Lösegeldforderungen entsprechend hoch zu schrauben. Der jährliche Schaden liegt alleine hierzulande im Milliardenbereich.
Als Gegenmaßnahme hatte Microsoft angekündigt, Makros zukünftig automatisiert genauer unter die Lupe zu nehmen und deren Ausführung zu blocken, sobald diese ein ungewöhnliches Verhalten zeigen, etwa Code aus dem Internet nachzuladen. Das entspricht praktisch einem Virenscanner innerhalb von Office.
Obwohl Microsoft mittlerweile jedem Windowsrechner einen brauchbaren Virenscanner spendiert, haben die Pläne für Office nicht nach den eigenen Vorstellungen funktioniert. Die Funktion wurde bis auf Weiteres eingestellt, da es zu Problemen in der Umsetzung gekommen sei.
Im Sinne der Sicherheit ist zu hoffen, dass das nicht das letzte Wort ist und die Programmierer es schaffen, Sicherheit und Komfort zu verbinden. Trotzdem gilt nach wie vor: Denken Sie an Ihre Backups!

Russland übernimmt Apple

…für etwa 12 Stunden. Dem bedeutenden russischen Anbieter Rostelecom ist es einen halben Tag lang gelungen, sich als Besitzer eines IP-Adressblocks auszugeben, der eigentlich Apple gehört. Dadurch wurde weltweit der für diese Adressen bestimmte Datenverkehr in das Netz Rostelecoms geleitet. Dadurch kam es für einen Teil der Apple-Nutzer zu Problemen beim Zugriff auf Dienste wie der iCloud. Inwieweit Rostelecom Apple-Nutzer dabei ausspioniert hat, lässt sich nicht unabhängig prüfen.
Dass das überhaupt möglich war, liegt am arglosen Umgang Apples mit den eigenen Adressen. Die Internetrichtlinien untersagen zwar Netzbetreibern, sich der IPs anderer zu bemächtigen. Offenbar hat sich Apple darauf verlassen, dass sich jeder daran hält. Seit vielen Jahren gibt es aber auch technische Mittel, um die Zugehörigkeit von Adressen zum eigenen Netz durchzusetzen, die Resource Public Key Infrastructure RPKI sowie die Route Origin Authorization ROA. Hier können digital signierte und von den IP-Vergabestellen geprüfte Zugehörigkeiten offiziell bekannt gegeben werden. Aus unbekannten Gründen verzichtet Apple darauf.
Das entspricht leider dem Bild, das bei Apples Umgang mit IP-Adressen generell zu sehen ist. So drängt Apple andere Netzbetreiber, sich auf möglichst kurzem Weg mit Apple zu verbinden und konfiguriert seine Systeme entsprechend offen vor. Dass diese Offenheit gleichzeitig Unsicherheit bedeutet, betrachtet man in Kalifornien scheinbar als weniger wichtig.
Möglicherweise setzt jetzt ein Umdenken bei den Verantwortlichen ein.

Neues von den Domains

.eu

die Europäische Kommission hat EURid für weitere fünf Jahre zum Betreiber der Endung .eu inklusive seiner griechischen und kyrillischen Varianten ernannt.
Gleichzeitig hat EURid eine Vereinbarung mit ICANN unterzeichnet, die der Förderung von Umlautdomains und besserer Unterstützung von Umlaut-Emailadressen dienen soll.

.fr

Die französische Registry Afnic hat angekündigt, Verstöße gegen die Registryrichtlinien zukünftig bereits bei der Registrierung eines Namens verstärkt ins Visier zu nehmen.
Dazu werden die Adressdaten des zukünftigen Domainbesitzers auf Existenz geprüft. Sollte es hier zu Unstimmigkeiten kommen, beginnt ein Nachweisverfahren, bei dem gezeigt werden muss, dass die Adresse tatsächlich gültig ist, etwa durch einen Handelsregisterauszug oder einer amtlichen Adressbestätigung. Sollte diese nicht innerhalb von sieben Tagen vorliegen, wird der Reservierungswunsch abgelehnt.

.kids

Die mit dem Erscheinen dieses Newsletters erhältliche .kids möchte ein sicherer Hafen für kindgerechte Webseiten werden. Dazu verpflichtet die Registry alle Inhaltsanbieter von ungeeigneten Materialien Abstand zu nehmen. Dazu gehören unter anderem Gewalt, Drogen, Pornografie und Glücksspiel. Bei Verstößen droht die Sperrung.

.ua

Die Tschechische Republik ist der Ukraine zur Seite gesprungen und migriert wichtige Teile der Registry-Infrastruktur aus dem Konfliktgebiet weg. Der Betrieb der .ua TLD wird damit weiterlaufen, selbst wenn sich die Situation vor Ort weiter verschlimmern sollte.

.za

Südafrikanischen Domainbesitzern stehen voraussichtlich erhebliche Nachweispflichten bevor. Die Registry hat beschlossen, dass .za Inhaber einen Identitätsnachweis erbringen müssen. Zudem erwartet die Registry von Domainanbietern wie Global Village einen Zugriff auf deren Infrastruktur. Wie genau dieser aussehen soll, ist noch nicht klar, aber hier könnte es potenziell zu Konflikten mit europäischer und nationaler Gesetzgebung kommen. Noch sind die Pläne aber nicht endgültig verabschiedet. Kritiker befürchten einen drastischen Domainschwund, sollten die Absichten wie angedacht umgesetzt werden.

Centralnic

Bei den von Uniregistry erworbenen TLDs .audio, .pics, .christmas, .guitars, .diet, .flowers, .game, .hosting, .lol und .mom leistet sich die Registry einen im Jahr 2022 außerordentlich peinlichen Lapsus. Offenbar sind die neuen Systeme nicht in der Lage, Umlaut-Domains in den Skripten Chinesisch, Deutsch, Japanisch und Kyrillisch zu unterstützen. Insgesamt seien aber nur 50 Domains betroffen. Centralnic scheint den Aufwand für die Unterstützung für unwirtschaftlich zu halten. Ob die genannten 50 Domains Bestandsschutz erhalten, ist noch unklar.

Mit freundlichen Grüßen,
Ihr Global Village Team