Newsletter April 2023

- Schwere Sicherheitslücke bei Office365
- Rufumleitung nach Nordkorea
- TikTok unter Beschuss
- Alibaba wird aufgespalten
- Neues von den Domains: .ai, .cr / .py, .dk, Google und .watches

Schwere Sicherheitslücke bei Office365

Forschern der Sicherheitsfirma Wiz ist es gelungen, administrativen Zugriff auf die Suchmaschine Microsoft Bing zu erhalten. Dies konnten sie nutzen, um Autorisierungsdaten des Azure Active Directory abzugreifen, die eigentlich dazu dienen sollen, Zugriffsberechtigungen für Office-Daten zu verwalten. Unter dem Strich gaben die Besucher von Bing unbemerkt ihre Dokumente für Dritte frei. Glücklicherweise handelte es sich in diesem Fall um die nicht böswillig auftretenden Forscher.
Nichtsdestotrotz sollten Administratoren stets sorgfältig abwägen, ob die Auslagerung in die Cloud für die jeweiligen Daten vertretbar ist. Wer auf eigene Server setzt, muss natürlich selbst Sorgfalt walten lassen, um die Systeme entsprechend abzuschotten. Der Fall demonstriert aber eindrücklich, dass ein Administrator bei Clouddiensten alles richtig einrichten kann und die eigenen Daten trotzdem nicht sicher sind.

Rufumleitung nach Nordkorea

Nutzer der Telefoniesoftware 3CX müssen aufpassen. Hackern, die mutmaßlich aus Nordkorea stammen, ist es scheinbar gelungen, Teile der PC-Version der Software auf Seiten des Herstellers auszutauschen. Sie funktioniert weiterhin normal, aber im Hintergrund verbindet sie sich mit Servern des Angreifers und verseucht den lokalen Rechner. Dadurch können die Hacker nicht nur Telefonate mithören, sondern haben Vollzugriff auf die Maschine des Betroffenen inklusive aller Dokumente und Daten.
Wer 3CX einsetzt, sollte dringend ein Update auf die aktuellste Version durchführen, in der die Sicherheitslücke geschlossen ist. 3CX hat noch keine Auskunft erteilt wie es zu dem Vorfall kommen konnte.

TikTok unter Beschuss

Schwere Zeiten für Bytedance, den chinesischen Besitzer von TikTok. Zwar hat die Videoplattform einen kometenhaften Aufstieg hinter sich und ist in vielen Ländern die Nummer 1 bei jungen Internetnutzern. Gleichzeitig erfährt Bytedance scharfen Gegenwind. Vor allem europäische und U.S.-amerikanische Politiker fürchten, dass Nutzer durch China ausspioniert und manipuliert werden.
Nun musste TikTok-Chef Shou Chew vor einem U.S. Ausschuss drastische Maßnahmen gegen seinen Konzern abwenden. Die Anhörung glich aber eher einem Schauprozess. Chew musste seine 10-seitige Erklärung erheblich kürzen, da er nur 5 Minuten Redezeit bekam. Auch im Verlauf der Anhörung kam er selten zu Wort, wurde dabei aber häufig unterbrochen. Der häufig geäußerte Vorwurf sowohl von Demokraten als auch Republikanern: TikTok sei ein verlängerter Arm der chinesischen Regierung. Beweise dafür präsentierten die Politiker nicht. Die nicht weniger invasive Plattform Youtube war in der Sitzung kein Thema.

Alibaba wird aufgespalten

Eines der größten Unternehmen Chinas steht vor seiner Aufspaltung. Alibaba, Betreiber der weltgrößten B2B, C2C und B2C Plattformen und einer der größten Cloudanbieter bringt 220 Milliarden Dollar auf die Waage. Diese sollen nun in sechs in einer Holding organisierten Einzelfirmen unterteilt werden - ein in China außergewöhnlich unüblicher Vorgang. Dabei soll jede Sparte individuell am Kapitalmarkt operieren und beispielsweise Fremdkapital aufnehmen können.
Die Regierung bedrängt Alibaba bereits seit zwei Jahren. Firmengründer Jack Ma war wohl nicht linientreu genug. So war er für ein Jahr aus der Öffentlichkeit verschwunden und galt damit als der unerreichbarste Milliardär der Welt.
Zukünftig steht Topmanager David Zhang dem Konglomerat vor. Vermutet wird, dass er vor allem KI-Projekte vorantreiben wird.
An der Börse stiegen die Alibaba Aktien seit der Ankündigung um gut 15%.

Neues von den Domains

.ai

Die vielfach für ‚Künstliche Intelligenz' / ‚Artificial Intelligence' Domains genutzte Endung ist eigentlich die Länderendung der Anguilla-Insel. Diese wurde für zwei Wochen komplett vom Internet abgeschnitten, da das einzige datenfähige Unterseekabel beschädigt wurde. Auf bestehende .ai Domains hatte das keine Auswirkung, da die .ai Nameserver wie üblich weltweit redundant verteilt sind.

.cr und .py

Costa Rica und Paraguy unterstützen jetzt DNSSEC zur kryptographischen Absicherung von DNS-Daten.

.dk

Nicht-Dänen, die .dk Domains reservieren möchten, benötigen für Registrierungen eine Personalausweiskopie nebst aktuellem Lichtbild und eine Gas-, Strom- oder Telefonrechnung um sich gegenüber der Registry auszuweisen. Bei Firmen ist ein Handelsregisterauszug notwendig. Die Dokumente müssen auf Dänisch oder Englisch vorliegen oder entsprechend übersetzt sein.

Google

Der Suchmaschinenbetreiber bringt eine Reihe neuer TLDs online. .foo, .dad, .esq, .mov, .nexus, .phd, .prof und .zip starten am 03.04. in die Sunrise-Phase, am 03.05 in den ‚Early Access' und bereits am 10.05. in die ‚Für Alle' Phase.
Die Einführung von .zip war wegen der bekannten gleichlautenden Dateiendung umstritten. Eigentlich hatte ICANN die Einführung von TLDs, die technische Verwirrung auslösen könnten, untersagt.

.watches

Ab sofort können .watches Domains in der Sunrise-Phase für Markenbesitzer registriert werden. Am 31.05. folgt die ‚Early Access' Phase und die ‚Für Alle' Phase am 07.06. .

Mit freundlichen Grüßen,
Ihr Global Village Team