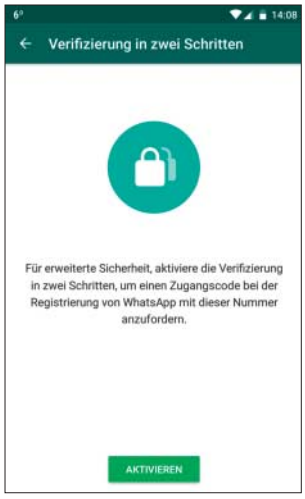
Sicherere Nutzerkonten bei WhatsApp

Mit einer neuen Funktion will WhatsApp das Kapern von Konten erschweren: Bei der „Verifizierung in zwei Schritten“ handelt es sich um die Einführung eines optionalen Passworts. Bisher waren WhatsApp-Konten lediglich an die Telefonnummer gekoppelt. Bei der An- oder Ummeldung einer Nummer wird dem Nutzer eine Einmal-PIN per SMS zugesandt, um zu bestätigen, dass er die entsprechende Nummer auch wirklich innehat. Deshalb braucht der Nutzer lediglich eine SIM-Karte, die zu der entsprechenden Nummer passt, um WhatsApp auf einem Gerät zu nutzen.

Dieser Vorgang ist für die Nutzer sehr bequem und hat bei der enormen Verbreitung des Messengers zweifellos eine Rolle gespielt. Er stellt aber auch ein Risiko dar, da Unbefugte das WhatsApp-Konto übernehmen können, falls sie es schaffen, die Kontrolle über die Telefonnummer des Nutzers zu erhalten. Das funktioniert, indem sie die Nummer auf einem anderen Gerät erneut aktivieren und die Aktivierungs-SMS abfangen – etwa über eine zweite SIM-Karte für dieselbe Nummer oder durch einen Angriff auf das SS7-Protokoll. Im August waren im Iran über einen dieser Wege Konten des WhatsApp-Konkurrenten Telegram kompromittiert worden.

Wer die optionale Verifizierung in zwei Schritten aktiviert, muss einen sechsstelligen Code festlegen, der bei der Kontoverifizierung der dazugehörigen Telefonnummer abgefragt wird. Wird eine Aktivierung eines WhatsApp-Kontos mit Zwei-Schritt-Verifizierung auf einem neuen Gerät durchgeführt, bei der der sechsstellige Code nicht eingegeben wurde, schlägt diese fehl, falls das Konto in den letzten sieben Tagen benutzt wurde. Nach sieben Tagen kann das Konto wieder ohne den zusätzlichen Code aktiviert werden, allerdings löscht WhatsApp dann alle nicht zugestellten Nachrichten. 30 Tage nach der letzten Nutzung können auch andere Nutzer die Telefonnummer erneut bei WhatsApp verifizieren – in diesem Fall wird das alte Konto komplett gelöscht. Die neuartige Verifizierung schützt also vor Missbrauch eines aktiven Kontos, blockiert aber keine Telefonnummern.



Die „Verifizierung in zwei Schritten“ schützt den WhatsApp-Account durch einen zusätzlichen Passcode vor Missbrauch.

Man schaltet die doppelte Kontoverifizierung unter „Einstellungen / Account / Verifizierung in zwei Schritten“ ein. Momentan ist diese Funktion allerdings nur für Betaversionen von WhatsApp verfügbar. Wann sie allen Nutzern zur Verfügung gestellt wird, ist unklar. Optional können Nutzer eine E-Mail-Adresse angeben, über die sie die zusätzliche Sicherheitsmaßnahme wieder deaktivieren können. Hat man den sechsstelligen Code vergessen, ist dies die einzige Möglichkeit, das eigene WhatsApp-Konto auf einem anderen Gerät unbeschadet zu reaktivieren. *(fab@ct.de)*

Multi-WAN-Router mit LTE-Option

Der Multi-WAN-Router TDT VR2020 soll dank seines Metallgehäuses auch für den Einsatz in Industrieanlagen taugen. Die bindet er per Vectoring-VDSL, Gigabit-Ethernet und optional LTE-Mobilfunk ins Internet ein.

Seine Multi-WAN-Router der VR2020-Reihe bietet der bayerische Hersteller TDT in zwei Ausführungen an: Das 422 Euro teure D-Modell besitzt ein Vectoring-fähiges xDSL-Modem und einen Gigabit-Ethernet-Port für die WAN-Verbindung. Die LD-Variante für 928 Euro hat zusätzlich ein LTE-Mobilfunkmodul (CAT3, max. 100/50 MBit/s Down-/Uplink, Band 1/3/7/8/20) mit Dual-SIM-Slot. Bei Ausfall der xDSL-Verbindung schalten die Router auf den alternativen Internetzugang um (Failover, auch per VRRP); Load Balancing ist nicht vorgesehen.

Die vier Fast-Ethernet-LAN-Ports lassen sich individuell für verschiedene Subnetze konfigurieren. Dank des Weitbereichseingangs – optional mit Klemmen statt Hohlstecker – kann man die VR2020-Router auch aus industrieüblichen 24-Volt-Netzen speisen. Softwareseitig gibt es die in dieser Klasse üblichen Managementzugänge: HTTPS, SSH, SNMP und TR-069 über einen TDT-Auto-Configuration-Server (ACS). Die integrierten VPN-Server für IPsec und OpenVPN bedienen bis zu 30 Tunnel; auf Client-Seite sollen beliebige IPsec-Tools, Softether und der OpenVPN-Client funktionieren. *(ea@ct.de)*

Nebula steuert Firmennetze

Als Ergänzung zu seinen physischen WLAN-Controllern hat der taiwanische Netzwerkhersteller Zyxel die Cloud-Anwendung Nebula gestartet, die sich als Demo ausprobieren lässt (siehe c’t-Link). Der in Europa gehostete Dienst soll alle Geräte der gleichnamigen Baureihen (Nebula Access Points, Switches und Security Gateways) vollständig fernsteuern können. Zyxel verspricht „Plug and Play“ bei der Inbetriebnahme: Läuft auf dem Smartphone die Nebula-App, soll das Scannen des QR-Codes auf der Verpackung reichen, um ein Gerät ins eigene Cloud-Konto einzubinden. Fachhändler können laut Zyxel auch Netze mehrerer Kunden verwalten (Multi-Site-Betrieb). *(ea@ct.de)*

Nebula-Demo: ct.de/yn2c