EDITORIAL

Digitale Lebensadern

Resilienz ist ein Schlagwort unserer Zeit – und war übrigens auch das zentrale Designziel des Internets. Selbst im Fall eines Kriegs und großteils zerstörter Infrastruktur sollten die Daten fließen. Inzwischen scheint diese Vorgabe in weiter Ferne. Wir erinnern uns an das Flughafenchaos in Frankfurt Mitte Februar, als auf einer Baustelle der Deutschen Bahn ein Glasfaserstrang der Telekom durchtrennt wurde. Ein Schelm, wer Absicht dahinter vermutet.

Mit Resilienz schien es hier jedenfalls nicht weit her gewesen zu sein. Und auch in der Cloud reichte schon ein falscher Konfigurationsbefehl, um Microsoft 365 und Azure in die Knie zu zwingen. Unser Chefredakteur hatte diesen kuriosen Vorfall von Ende Januar in seinem März-Editorial aufgegriffen.

Unsere Gesellschaft ist hochgradig vernetzt und von ihren digitalen Lebensadern abhängig. Fällt die Internetanbindung, die Cloud oder eine Kommunikationsplattform wie Teams aus, drehen viele Mitarbeiter in Unternehmen Däumchen. Hier hilft zuallererst Redundanz, auch wenn diese Geld und Aufwand kostet. Daneben steht und fällt die Zuverlässigkeit der IT-Umgebung mit deren Absicherung – auch und gerade in der Cloud.

Das nach wie vor größte IT-Sicherheitsrisiko sind Ransomware-Attacken, die täglich Firmen und Behörden lahmlegen. Und es ist nur eine Frage der Zeit, bis nicht mehr "nur" Server und Clients in Geiselhaft gehen, sondern vernetzte und womöglich kritische Maschinen. Die Bedrohung reicht so weit, dass die US-Regierung in ihrer aktuellen Cybersecurity-Strategie vom März Ransomware als Bedrohung der nationalen Sicherheit einstuft.

Auch Clouds sind nicht vor solchen Angriffen gefeit. Wir zeigen Ihnen in diesem Sonderheft, wie Sie Microsoft Azure, Amazon Web Services und die Google Cloud Platform sicher administrieren und zugleich in lokalen virtuellen Umgebungen Angreifer auf das Abstellgleis schicken. Kein leichtes Unterfangen angesichts schwer greifbarer, dynamischer Workloads, die zwischen Servern sowie dem lokalen Rechenzentrum und der Wolke hin- und herwandern. Ein zentraler Baustein ist daher Zero Trust, wie Klaus Bierschenk ab Seite 106 darlegt. Ebenfalls immer wichtiger wird die Automatisierung von IT-Security, die Martin Loschwitz ab Seite 173 beleuchtet.

Bleibt uns noch, unseren imaginären Hut vor den Technikern in der Ukraine zu ziehen, die unter Einsatz ihres Lebens die dortige Kommunikation in den Kriegswirren am Laufen halten.

Eine aufschlussreiche Lektüre wünschen

Daniel Richey John Pardey Lars Nitsch