»Backup, Backup, Backup!«

Das Datenrettungsunternehmen Attingo sorgt seit mehr als 24 Jahren für professionelle Datenwiederherstellung und kümmert sich um defekte Festplatten und SSD-Datenträger, ausgefallenen RAID- und Storage-Systeme, Speicherkarten und USB-Sticks. Dass das Thema aber nach wie vor zu wenig in den Management-Ebenen präsent ist, weiß Geschäftsführer Markus Häfele.

Wie hoch ist das Bewusstsein heimischer Unternehmen Ihrer Einschätzung nach beim Thema Security bzw. Datensicherung?
Auch wenn ich damit wirtschaftlich gegen uns spreche, fürchte ich als Techniker gesehen, dass das Thema Cybersecurity vor allem in den Mangement-Ebenen im KMU-Bereich trotz zahlreicher Vorfälle in den letzten Monaten und Jahren nach wie vor unterrepräsentiert ist. Das liegt zum einen an irreführenden Marketing-Versprechungen von so manchem Software- bzw. Hardware-Lieferanten, die naturgemäß auf gewisse Gefahrensituationen nicht ausreichend hinweisen, andererseits aber auch an fehlendem technischen Verständnis von komplexen Zusammenhängen und daraus resultierenden Einfallsvektoren. Auch wenn in früheren Zeiten der Technik-affine Neffe die Firmen-IT nebenher betreut hat, ist es in der immer vernetzteren Welt doch ratsamer einen professionellen Dienstleister zu rate zu ziehen um sein Netzwerk abzuzhärten. Denn man muss sich auch bewusst sein, dass man sich nicht hundertprozentig vor jeglichem Angriff bzw. Ausfall schützen kann, sondern auf den Tag X nur bestmöglich vorbereitet sein kann, damit dadurch kein Schaden entsteht.

Markus Häfele ist Geschäftsführer von Attingo Datenrettung.

Hat sich hier in Zeiten der Krise etwas geändert?
Gleich in mehrerlei Hinsicht haben sich durch die Pandemie ungünstige Veränderungen für die IT-Infrastruktur ergeben. Durch die plötzliche Umstellung auf Home Office kamen in vielen Fällen private PCs zum Einsatz, die dann über VPN-Zugänge direkt ins Firmennetz eingegliedert worden sind, aber mitunter einem weitaus geringeren Schutzniveau ausgesetzt waren, da sie über unzureichend Virenschutz und mangelnde (Hardware)Firewall im Heimnetz verfügen oder auch von minderjährigen bzw. unerfahrenen Mitnutzern »misshandelt« werden. Etwaige auf den Büro-PCs eingerichtete (automatische) Backups verliefen im Sand, da sich die Daten nun auf anderen Computern ansammelten, eine vielleicht noch rasch gekaufte externe Festplatte zur Speicherung und dem Transport der Firmendaten unterliegt im Privathaushalt aber auch einer überdurchschnittlichen Fliegkraft.
Ein weiterer Punkt liegt in unzureichendem Monitoring von Systemausfällen. Wenn Server oder NAS im Büro zu piepsen beginnen, hat das früher bestimmt ein Mitarbeiter wahrgenommen, wenn aber nun alle im Home Office sitzen, bekommt eventuell niemand den Festplattenausfall mit. Zu guter Letzt ist das IT-Budget in Kri-

senzeiten nach wie vor einer derjenigen Posten, die gerne als erstes gekürzt werden. Und auch Phishing- bzw. Ransomware-Angreifer wissen dank Social Engineering ganz genau, wem sie in wessen Namen eine gefälschte Mail zukommen lassen müssen, da mangels persönlicher Kontakte der Austausch auch von Arbeitsanweisungen auf E-Mail-Basis umgestellt worden ist und haben somit leichteres Spiel.

Welche sind derzeit die größten Security-Bedrohungen für Unternehmen?

Auf Platz eins steht hier inzwischen bestimmt die Bedrohung durch Erpressungen – und zuletzt auch immer mehr Entführung (also das Absaugen und Veröffentlichen) – von kritischen Firmendaten. Durch vermehrten Einsatz von oftmals nicht updatebaren IoT-Devices, aber auch eventuell gar nicht genutzten Services von NAS-Servern, entstehen auch immer mehr Lücken im Netzwerk – vor allem wenn diese Geräte über eine Cloud über direkte offene Port-Zugriffe verfügen »müssen« und nicht in einem separeten Netz abgekapselt sind.

Zwei weitere Dauerbrenner sind aber nach wie vor Datenverlust, einerseits durch physische Ausfälle von Datenträgern in Arbeitsplätzen oder Server-Anlagen, andererseits aber auch durch Diebstahl/Verlust von unverschlüsselten Geräten, sowie der Faktor Mensch in jeglicher Hinsicht: Mitnahme oder Löschung bei gekündigten Mitarbeitern, fatale Entscheidungen im Falle eines aufkommenden Datenverlustes ohne ausreichendes Backup aber auch die bereits erwähnten Phishing- und Malware-Links in gut gemachten Mails.

»Man kann sich nicht hundertprozentig vor jeglichem Angriff bzw. Ausfall schützen, sondern nur bestmöglich vorbereitet sein.«

Markus Häfele

Wie schütze ich mich richtig um nicht Kunde bei Ihnen zu werden?

Um konkret vor Datenverlust aus den verschiedensten Gründen geschützt zu sein, gibt es drei Möglichkeiten: Backup, Backup und Backup. Und zwar sollten es tatsächlich in der Tat gleich mehrere sein, denn es kann beispielsweise bei einem Wasserschaden oder Brand oder auch Einbruch den neben dem Produktivsystem stehenden Datenträger ebenso erwischen. Im Zuge einer Ransomware-Attacke könnten die Daten auf dem letzten Backup bereits verschlüsselt sein und der Datenbestand von einer Vorwoche noch intakt sein. Es ist somit auch immens wichtig, dass es Sicherungen gibt, die offline gespeichert werden und weder von Angreifern noch Umwelteinflüssen im Büro angreifbar sind. cb