SHUTTERSTOCK

USB-Stick: Er kann Computer glauben lassen, er sei eine Tastatur, und sendet Tastenkombinationen. Was, wenn es ungewöhnlich lange dauert, bis ein Vorgang abgeschlossen ist? Oft eine Frage von wenigen Sekunden.

Sinnlose Burggraben-Mentalität

Die Digitalisierung und die vermehrte Cloud-Nutzung haben neben neuen Geschäftsmodellen auch **neue Cyber-Einfallstore** geschaffen.

VOLKER RICHERT

Kürzlich hat eine Studie des Cybersecurity-Unternehmens Sophos gezeigt, dass nur schon von der grassierenden Erpressersoftware (Ransomware) betroffene Schweizer Unternehmen bis zu 239 000 Franken Lösegeld bezahlt haben. Zusätzlich fielen für die Wiederherstellung der Systeme durchschnittlich fast 1,6 Millionen Franken an – und es dauerte einen Monat, um den angerichteten Schaden und die Geschäftsunterbrechung zu beheben.

Dabei, fügt Sophos-Schweiz Chef Mirko Casarico an, zahlt gut ein Drittel der hiesigen Unternehmen Lösegeld, um ihre Daten zurückzubekommen, selbst wenn sie über andere Mittel zur Datenwiederherstellung verfügten, zum Beispiel über Backups. Diese Zahlen belegen laut Casarico, dass eine traditionelle Antivirus-Strategie oder einzelne und nicht integrierte Security-Inseln im Unternehmen nicht mehr ausreichen. «Die Cyberkriminellen wissen, wo die Schlupflöcher sind, und nutzen diese bei zunehmender Digitalisierung raffiniert aus.»

Dass die Digitalisierung die Angriffsflächen in Unternehmen verändert, weiss man auch beim IT-Dienstleister UMB. Es gehe darum, sie kontinuierlich zu verkleinern, erklärt Markus Kaegi, der bei den Experten für Business- und Technologietransformation als Business Lead Cybersecurity amtet. «Besonders wichtig ist, dass nicht nur die technischen Herausforderungen betrachtet werden, sondern auch diejenigen, die von den Prozessen ausgehen.» Denn wenn Geschäftsmodelle digitalisiert würden, veränderten sich Abläufe und möglicherweise Zuständigkeiten, was neue Risiken zur Folge haben könne, so Kaegi weiter.

In der digitalen und mobilen Welt, wo man die IT aus einer Cloud bezieht, seien Grenzen eben nicht mehr so einfach zu definieren. Allerdings könne, wer seine Cybersecurity-Maturität gründlich und wiederkehrend evaluiere, daraus relevante Tätigkeiten und Systeme ableiten.

Wie dieser Wandel konkret aussieht, illustriert Sophos-Mann Casarico am Beispiel der Entwicklungen unter den Stichworten Homeoffice und Remote-Arbeit via VPN-Lösungen. Denn für Security-Profis ist «das VPN eine problematische Technologie, simuliert sie doch ein langes Netzwerkkabel vom externen Rechner direkt in das digitale Herz des Unternehmens – weitestgehend ohne die Schutzmassnahmen, die man üblicherweise gegenüber Externen walten lassen würde», sagt Casarico.

Das Thema sei so brisant, weil eine VPN-Verbindung mit dem Firmennetz generell als vertrauenswürdig angesehen werde, obwohl sie Cyberkriminellen, die sich Zugang zu einem Homeoffice-Rechner verschaffen, Tür und Tor öffne. Ganz abgesehen davon «ist die Verwaltung einer VPN-Remote-Access-Lösung in einer modernen Umgebung sehr komplex, aufwendig und fehleranfällig», so der Security-Experte von Sophos.

Hohe Ansprüche an hybride Clouds

Noch akuter wird die Sicherheitsfrage bei Cloud-Diensten, mit denen Unternehmen viel von ihrer Infrastruktur auslagern. So fordere die Verlagerung der IT oder von Teilen davon in die Cloud eine Adaption der Sicherheitsstrategie und -architektur im Unternehmen, erklärt Cyrill Peter, der die Cyber Security & Defense Services bei der Swisscom leitet. Neben Compliance-Aspekten «müssen die jeweiligen Sicherheitsverantwortlichen im Unternehmen neue Massnahmen definieren, um das Sicherheitsniveau der Organisation in der Gesamtheit zu gewährleisten». Das sei insbesondere deshalb wichtig, weil «in den allermeisten Fällen mehrere Cloud-Anbieter involviert sind, sprich: hybride Formen üblich sind, bei denen die Workloads auf diversen Public und Private Clouds wie auch noch in traditionellen Umgebungen vorhanden sind». Dafür bedarf es einer breiten Palette an Sicherheitsmechanismen, die

Systeme sollten bei untypischem Verhalten schnell reagieren.

in eine Gesamtarchitektur integriert sein wollen. Gleichwohl, so Peter weiter, ist «die Wahrscheinlichkeit sehr hoch, früher oder später Opfer von Cyberkriminellen zu werden».

Umso wichtiger sei es, auf solch einen Ernstfall vorbereitet zu sein. Neben der Prävention zum Beispiel mit Firewalls im Netzwerk und mit Zwei-Faktor-Benutzerauthentisierung beim Datenzugriff gehören dazu auch Detection-Fähigkeiten beispielsweise aus einem Security-Operation-Center, um Cyberangriffe schnell zu erkennen und abzuwehren. Auch wenn es, so Peter, dennoch keine 100-prozentige Sicherheit gebe, könne man Angriffe und daraus resultierende Security-Incidents zumindest schnell unter Kontrolle bringen. Dafür müsse man aber in einer derart ausserordentlichen Stresssituation auf Cyber-Fachexpertise zurückgreifen können.

Peter spricht damit die sogenannten CSIRT-Experten (Computer Security Incident Response Team) an, die helfen, eine «Attacke zu bewältigen und die (Folge-) Schäden einzudämmen», wie er sagt. Die Anforderungen an CSIRT seien allerdings so hoch, dass sie in der Regel im Servicemodell aufgeboten werden, so Peter.

Mehr Zugriffe auf Unternehmensdaten

Armando Chiodi, der als Partner beim SAP-Berater Q-Perior den Security-Bereich leitet, verweist auf weitere Schwachstellen, die sich aus dem inzwischen immer wichtiger werdenden Datendurchgriff ergeben: «Heute greifen bei allen grösseren Unternehmen Kundinnen und Kunden direkt auf ihre Daten zu und bekommen auch immer mehr Selfservice-Möglichkeiten.» Die reichen vom Tracking von Bestellungen über das Ändern von Stammdaten und reichen bis zum klassischen E-Banking, bei dem der Kundschaft der Datenzugriff ebenfalls erlaubt ist.

Obwohl hier das Abkapseln der Systeme vom Internet nicht möglich ist, sollen die Daten und Systeme aber wie bisher geschützt werden, beschreibt Chiodi die Herausforderung. Ohne zusätzliche technische Massnahmen sei das nicht zu haben. Insbesondere gehe es um solche, «die sicherstellen, dass die Kundinnen und Kunden diejenigen sind, für die sie sich ausgeben – und das nicht nur beim ersten Anmelden, sondern bei jedem weiteren Zugriff». Der Q-Perior-Experte erinnert an Lösungen nach dem Zero-Trust-Prinzip, das jedes nicht begründete Vertrauen in einen Datenzugriff ausschliesst.

Zudem verweist er auf einen vielfach übersehenen Bereich: das fehlende Monitoring der Systeme. Dass sich Angreifer längst in ihren Systemen tummeln, merken Unternehmen oft erst, wenn Daten gelöscht oder verschlüsselt sind. Deshalb sei es «wichtig, Systeme und Prozesse zu betreiben, die die Systemlandschaft auf untypisches Verhalten hin überwachen und schnell reagieren», so Chiodi.

Interessant ist, dass Stefan Dettwiler, Chef des auf KMU spezialisierten IT-Service- und Cloud-Dienstleisters Exxo, sich die ablehnende Haltung von Sophos gegenüber der VPN-Nutzung nicht zu eigen macht. Auch wenn es wie «bei den meisten IT-Themen auch bei der Cloud-Auslagerung keine ‹One size fits all›-Lösung für Unternehmen» gebe, müsse ein Firmennetzwerk oder -portal doch mit einer Firewall und guten Antivirensystemen geschützt werden. Zudem sei der Internetverkehr via VPN als verschlüsselte Netzwerkverbindung zu nutzen. Überdies empfiehlt neben einer Multifaktorauthentifizierung, die Infrastruktur auf dem aktuellen Stand zu halten und sämtliche Daten mit einem Backup-Konzept zu sichern. Dabei sei für über das Internet zugängliche Kundenportale und Webapplikationen zusätzlich eine Web Application Firewall einzusetzen, die den Traffic überwacht und ihn bei Bedarf blockiert.

Die hohe Komplexität meistern

Schon diese blosse Aufzählung spiegle die hohe Komplexität der IT-Systeme und -Sicherheit, ergänzt Dettwiler. Hier erlaube es die Auslagerung in die Cloud, wenn sie mit den modernsten und wirksamsten Schutzmassnahmen ausgerüstet ist, «in den meisten Fällen die eigene IT-Sicherheit» zu erhöhen. Konkret verweist er auf die so mögliche professionelle Unterstützung auch bei Authentifizierungs- sowie Berechtigungsproblemen und falsch konfigurierten Datenspeichern, welche die schwächsten Glieder einer durchgängigen Cloud-Sicherheit seien. Davon abgesehen erinnert Dettwiler daran, dass bei der Cloud-Nutzung der Datenspeicherort bedeutsam wird. Für besonders kritische und vertrauenswürdige Daten ist laut dem Exxo-Chef ein reiner Schweizer Cloud-Provider durchaus sinnvoll.