«Unternehmen bemerken den Angriff häufig erst, wenn es zu spät ist»

Der IT-Markt-Cashman will dem Handel helfen, mit den nötigen Produkt- und Fachkenntnissen besser zu beraten. In diesem Cashman: die Gefahren von Ransomware und deren Eindämmung mit den Firewall-Lösungen von Zyxel. Auskunft gibt Frank Studerus, Managing Director der Studerus AG. Interview: David Klier

Weshalb sprechen alle momentan von Ransomware?
Frank Studerus: Es gab in letzter Zeit vermehrt Meldungen von Ransomware-Fällen, und viele vermeintlich sichere grössere Organisationen wie etwa öffentliche Verwaltungen oder Kliniken zählten zu den Opfern. Ransomware trat in der Vergangenheit vor allem in den USA auf. Seit Beginn dieses Jahres häufen sich die Fälle jedoch auch in unseren Breitengraden. Ransomware wird für immer mehr Unternehmen zu einer potenziellen Bedrohung.

Wie funktioniert Ransomware, und wie gross ist der dadurch angerichtete Schaden?
Ransomware infiltriert den Computer und verschlüsselt einzelne Files oder legt den Rechner ganz lahm. Nur mit der Zahlung eines vom Erpresser geforderten Geldbetrages werden diese Daten wieder entschlüsselt. Die Funktionsweise von Ransomware ist simpel. Der Nutzer erhält eine infizierte E-Mail, eine sogenannte Spear-Phishing-E-Mail. Wenn er diese E-Mail öffnet, wird automatisch eine infizierte Datei ausgeführt, welche die Daten des Nutzers verschlüsselt. Im Anschluss erscheint auf dem Bildschirm eine Erpressernachricht mit einer Lösegeldforderung für das Entschlüsseln der Daten. Meist ist diese in der Internetwährung «Bitcoins» zu bezahlen, die keinen Rückschluss auf den Zahlungsempfänger zulässt. Die betroffenen Daten können während dieser Zeit nicht oder nur eingeschränkt erreicht werden. Dies kann massive Folgekosten nach sich ziehen, besonders dann, wenn die verschlüsselten Dateien neu erstellt werden müssen. Dazu kommt ein Imageschaden, wenn ein solcher Erpresserfall an die Öffentlichkeit gelangt.

Wie merkt ein Unternehmen, dass es angegriffen wurde?
Häufig merkt das betroffene Unternehmen den Angriff erst, wenn es schon zu spät ist. Ein falscher Klick genügt. Das Schadprogramm führt dann die Verschlüsselung der Daten durch und nutzt dabei die dem Mitarbeiter freigegebenen Laufwerke. Es gibt einige typische Begleitumstände, die auf einen Fall von Ransomware hindeuten: Nutzer erhalten meist die Option, fünf Dateien zu entschlüsseln. Die Lösegeldfrist beträgt häufig etwa 100 Stunden und die Lösegeldsumme bewegt sich zwischen 500 und 1000 Franken. Viele Unternehmen bezahlen die Summe deshalb.

Welche Vorkehrungen kann man treffen, um sich vor Ransomware zu schützen?
Wichtig ist, alle möglichen Security-Vorkehrungen auszuschöpfen. Man muss auf ein komplettes Security-Konzept zurückgreifen können. Eine solide Firewall in Kombination mit Unified-Threat-Management-Services sorgt für eine vielschichtige Abwehr. Zyxel bietet hier mit der USG-Serie ein umfangreiches Portfolio. Ausser den UTM-Services ist es für die Sicherheit eines Systems unabdingbar, immer wieder Back-ups wichtiger Daten durchzuführen und sämtliche Systeme auf dem neuesten Stand zu halten. Nicht zu unterschätzen ist der vorsichtige Umgang mit seinen Daten im Web.

Was sind die Vorteile der Zyxel-UTM-Services im Kampf gegen Ransomware?
Früher haben Unternehmen gezögert, UTM einzusetzen oder sie zumindest in vollem Umfang zu installieren. Bedenken wegen der Performance waren hier stets der Hemmschuh. Heutzutage ist das dank der leistungsfähigeren Prozessoren kein Thema mehr. Auch die Häufung von Ransomware-Fällen hat in dieser Hinsicht Veränderungen gebracht und neue Chancen für Händler geschaffen. Mit den UTM-Services aus einer Hand bietet Zyxel einen «All-in-One»-Schutz, was ein grosser Vorteil gegenüber vielen anderen Herstellern ist. Das Security-Portfolio von Zyxel ist sehr umfassend und bietet vom Kleinstunternehmen bis zum mittleren KMU die richtige Lösung. Mit One Security bietet Zyxel ein Portal, das Hilfe bei der Wahl des richtigen Security-Produktes sowie beim Einrichten von UTM-Services ermöglicht und Infos zur aktuellen Bedrohungslage liefert. Nicht zu vernachlässigen sind die Cross-Selling-Möglichkeiten, da ein Fachhändler mit Zyxel nicht nur Firewalls, sondern auch Switches und WLAN-Produkte aus einer Hand anbieten kann. Das Zyxel-Partnerprogramm bietet den Händlern zudem eine starke Unterstützung für die erfolgreiche Marktbearbeitung.

Frank Studerus, Managing Director des Netzwerk-Distributors Studerus.