«Cybersecurity ist Chefsache – Kontrolle auch!»

Jüngste Cyberangriffe zeigen, wie nachlässig einige Firmen sind. Es mangelt an einfachsten Vorkehrungen. Cyrill Brunschwiler berichtet über die Vorfälle und beschreibt, was einen minimalen Schutz ausmacht.

Herr Brunschwiler, kürzlich haben europäische Sicherheitszentren vor einer Angriffswelle gewarnt. Worum ging es genau?

Es ging um Angriffe, bei denen in grossem Stil Serversysteme abgeschaltet und verschlüsselt wurden. Zuerst wurde der Vorfall von einem Cloud-Provider in Frankreich öffentlich rapportiert. Es wurden bekannte Schwachstellen in der Virtualisierungslösung VMware ESXi ausgenutzt. Dieses Produkt wird von zahlreichen Cloud-Kunden und IT-Dienstleistern in Eigenregie betrieben. Aufgrund der Erkenntnisse realisierten die europäischen Sicherheitszentren, dass es auch andere betreffen könnte und sprachen die Warnung aus.

Was bedeutet VMware ESXi?

Es handelt sich um eine Virtualisierungsplattform, die meist verwendet wird, um Kosten zu sparen. Wer heute in eine Hardware investiert, lässt darauf oft nicht nur einen Server, sondern mehrere laufen. So kann man sich die Rechen- und Speicherkapazität für mehrere Systeme teilen.

Was war genau das Problem?

Das Produkt hatte eine Schwachstelle, die vom Hersteller im Februar 2021 durch ein Update behoben wurde. Wer den entsprechenden Patch seit zwei Jahren nicht eingespielt hat, ist verwundbar.

Überrascht Sie diese Angriffswelle?

Das Erstaunliche ist, dass der verwundbare Dienst gar nicht im Internet erreichbar sein dürfte. Hinzu kommt, dass er zumeist nicht benötigt wird und abgeschaltet werden könnte. Es gibt also offensichtlich immer noch Betreiber, die unnötigerweise Systeme im Internet exponieren und es obendrauf versäumen, Updates einzuspielen.

Was haben die Angreifer gemacht?

Die Angreifer vergleichen jeweils das Update mit der ursprünglichen Software und erkennen so, welche Lücke geschlossen wurde. Wenn neue Patches herauskommen, ist folglich schnell bekannt, wo das Problem liegt. Im konkreten Fall dauerte es trotzdem sehr lange, bis dann die Welle wirklich anrollte. Die Angreifer haben dann über die Lücke ein eigenes Programm ausgeführt und konnten so die Server stoppen und deren Daten verschlüsseln.

Was sind die Schäden? Sind Daten gestohlen worden?

Teils waren Systeme nicht mehr lauffähig oder wichtige Daten waren partiell verschlüsselt worden. Zwar ist dies nur ein Teilausfall, allerdings ist auch dieser sehr ärgerlich. Bei allen Fällen, die wir auf dem Tisch hatten, konnten wir glücklicherweise keinen Datenabfluss erkennen. Viele sind mit einem blauen Auge davongekommen. Die Schäden hätten weit grösser sein können – hätten es sich die Angreifer ein bisschen genauer überlegt und ihr Tool besser getestet.

KMUSCHUTZ.CH FASST DIE WICHTIGSTEN SCHUTZMASSNAHMEN ZUSAMMEN

Egal wie es letztlich ausging – es wäre zu verhindern gewesen?

Absolut. Man hätte einfach den Patch einspielen sollen und die Firewall schliessen müssen. Eines von beidem hätte sogar gereicht.

Wo sollte man den Hebel ansetzen?

Es ist Aufgabe der Geschäftsleitung festzulegen, was von der IT bezüglich der Cybersicherheit erwartet wird. Es muss einem Unternehmer klar sein, welche Prozesse von der IT abhängen. Den Informatikern kann man im konkreten Fall vorwerfen, dass sie die Sorgfaltspflicht verletzt haben. Die Geschäftsleitung hat es aber auch versäumt, einfachste Kontrollen anzuordnen.

Zum Schutz vor Hackern haben Sie die Initiative «Swiss Cyber Defence-DNA» ins Leben gerufen …

Richtig. In einem Leitfaden wurde zusammen mit namhaften Herstellern und reputablen Schweizer Unternehmen festgehalten, wie sich KMU effizient gegen Cyberkriminalität schützen können. Ausschlaggebend hierfür war die Erkenntnis, dass sich viele KMU eine einfache Hilfestellung wünschen, wie sie gegen Ransomware vorsorgen können.

Welche Punkte erachten Sie als besonders wichtig?

Das Sechs-Punkte-Programm auf dem Portal kmuschutz.ch führt ganz pragmatisch die wichtigsten Dinge, die zu tun sind, zusammen. Diese reichen vom unveränderbaren Backup über den aktuellen Schutz vor Schadsoftware, wie Virenscanner und Firewall, bis hin zur Segmentierung und Absicherung von Netzwerken. Aber auch die Hard- und Software aktuell zu halten, ist von Bedeutung. Ein weiteres Ziel liegt darin, einen Notfallplan im Unternehmen zu erstellen – alles Massnahmen, die den Fokus haben, Angriffe zu verhindern, Schäden zu limitieren und ein KMU am Leben zu halten.

IM INTERVIEW
Cyrill Brunschwiler
Compass Security Schweiz
Trägerschaft Swiss Cyber Defence-DNA
www.kmuschutz.ch