Tages-Anzeiger

FOKUS.
BUSINESS CHALLENGES

EINE PUBLIKATION VON SMART MEDIA

BRANDREPORT • MOUNT10 AG

So schützen sich KMUs vor virtuellen Bedrohungen

Noch immer sind viele KMUs nur ungenügend vor Cyberangriffen geschützt.
Wie kleine und mittlere Unternehmen sicherer gemacht werden können, weiss Thomas Liechti, CEO der Mount10 AG.

Thomas Liechti
CEO Mount10 AG

Was ist Ransomware?
Ransomware ist der Überbegriff für eine spezielle Art von Computerviren, die man sich via E-Mail-Anhängen, USB-Sticks oder auch bei Besuchen auf unsicheren Webseiten einfangen kann. Diese Viren lassen sich aber nicht einfach so erkennen und entfernen, sondern sie verschlüsseln im Hintergrund unbemerkt alle Daten und machen sie komplett unbrauchbar und unlesbar, bevor man den Virus überhaupt erkennt.

Wenn man den Virus erkennt, ist es meist zu spät und man ist mit einer Erpressung konfrontiert. Die Firma wird genötigt, innerhalb kurzer Zeit dem Erpresser Bitcoins zu bezahlen, ansonsten erlaubt er keine Entschlüsselungsmöglichkeit. Ein Lösegeld zu zahlen, ist aber ausdrücklich nicht empfohlen. Damit unterstützt man zukünftige kriminelle Machenschaften.

Wie schütze ich mich vor diesen Viren?
Man kann sich nicht zu 100 Prozent davor schützen, die einzige Möglichkeit, ein Desaster zu verhindern, ist eine gute Vorbereitung.

Was meinen Sie genau mit guter Vorbereitung?
Eigentlich ist es bei der virtuellen Bedrohung gleich wie bei einer physischen. Je besser man auf den Fall der Fälle vorbereitet ist, desto eher kann man den Angriff unbeschadet überstehen. Genau dafür haben wir zusammen mit Industriegrössen die Swiss Cyber Defence – DNA Initiative lanciert. Dieser Leitfaden ist kostenlos und hilft KMUs sich pragmatisch und möglichst einfach gegen Cyber-Risiken zu wappnen. Von der Industrie, für die Industrie.

Kann ein KMU das selbst umsetzen?
Grundsätzlich kann es das schon, aus Gründen der Erfahrung und des tieferen Know-hows sollte es aber mit einem oder mehreren spezialisierten Umsetzungspartnern für die einzelnen sechs Massnahmen der SDC-DNA zusammenarbeiten. Diese sind auf der kmuschutz.ch-Seite unter den jeweiligen Massnahmen nach Region ersichtlich.

Sind KMUs denn überhaupt lohnende Angriffsziele?
Ob es sich lohnt oder nicht, ist grundsätzlich für die Cyber-Kriminellen nicht von anfänglicher Relevanz. Die Frage ist eher, wie einfach ist das Ziel zu knacken ist. Da es für die Hacker kaum namhaften Aufwand generiert, werden einfach mal alle Ziele angegriffen.

Aus Sicht der KMUs, kann es aber nur schon sehr bedrohlich werden, wenn alle Kunden- und Projektdaten nicht mehr vorhanden sind, noch unangenehmer wird es, wenn Finanzdaten oder gar Intellectual Property Daten zerstört werden. Wenn dann noch Produktionssysteme unwiderruflich zerstört sind und die Fabrikation stillsteht, dann wird's sehr eng. Eine der entscheidenden Fragen, die man sich in der Vorbereitung stellen muss, ist: Welche Daten und Systeme sind kritisch oder gar überlebenswichtig?

Muss es denn wirklich sein, sich auch noch damit zu befassen?
Leider ja, zum Wohle der Firma, der Mitarbeitenden, deren Familien und auch der Aktionär:innen ist dies leider unumgänglich.

“ Wenn man den Virus erkennt, ist es meist zu spät und man ist mit einer Erpressung konfrontiert.