Den Profi fragen!

Geschichten aus dem Minenfeld der Microsoft-Lizenzierung

Kürzlich bei der VENDOSOFT: Markus Seirer spricht mit dem besorgten IT-Leiter eines Pharmaunternehmens. Es war in der Vergangenheit Opfer eines Cyber-Angriffs. Mit der anschließenden Entscheidung für die E5-Pläne von Microsoft hatte man sich in Sicherheit gewogen. Nun hat Herr Dachser* in der Fachpresse gelesen, dass Microsoft 365 immer mehr zum Ziel von Cyberkriminalität wird. Unter anderem soll der Identitäts- und Informationsschutz ausgehebelt werden können, der diese Pläne vergleichsweise sicher macht. Alarmiert fragt er bei seinem CSP-Provider nach. Markus Seirer vom Microsoft Gold Partner VENDOSOFT gibt Antworten.

> Als Markus Seirer den Anruf von Herrn Dachser entgegennimmt, hat er gerade erst die Neuigkeiten der Black Hat aufgesogen, der wichtigsten internationalen Konferenz für Cyber Security. In diesem August befasste sie sich unter anderem mit den Sicherheitsrisiken für Microsoft 365. Weltweit nutzen 300 Millionen Geschäftskunden Microsoft-Produkte zur Erstellung von Dokumenten, zum Arbeiten in Teams, dem Datenaustausch oder zur Datenanalyse. Die dabei entstehenden Datenmengen werden zunehmend nicht mehr auf firmeneigenen Serverplattformen gespeichert, sondern in der Cloud. Das ruft Cyberkriminelle auf den Plan.

Hacker kennen die Schwachstellen besser als jeder Administrator

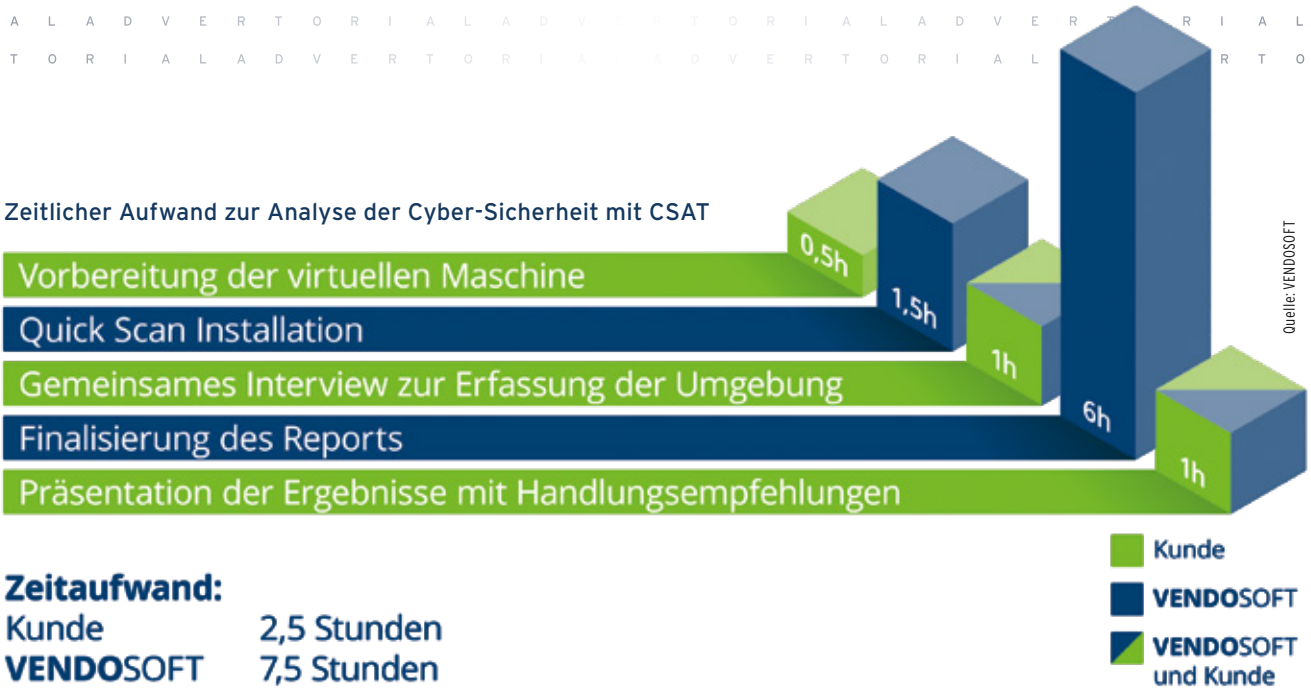
Regelmäßig werden im Rahmen von Ransom-Attacken Millionenbeträge von Unternehmen erpresst. Andere Hackergruppen handeln im Auftrag von Staatsregierungen. „Da geht es dann um Industriespionage und Datenklau“, erklärt Markus Seirer. Um das zu verhindern, verwenden Software-Hersteller wie Microsoft viel Zeit, Geld und Mühe darauf, die angebotenen Systeme sicher zu machen. Doch auch die Hackerszene bedient sich bestens ausgebildeter Programmierer und ent-

*Name auf Wunsch des Kunden geändert

Analyse des Cyber Security Assessment Tools von VENDOSOFT

Quelle: VENDOSOFT

ADVERTORIAL ADVERTORIAL ADVERTORIAL ADVERTORIAL ADVERTORIAL ADVERTORIAL



Zeitaufwand:

Kunde	2,5 Stunden
VENDOSOFT	7,5 Stunden

wickelt immer raffiniertere Methoden, um unbemerkt in Firmennetzwerke einzudringen. Und sie weiß definitiv mehr über die Schwachstellen von Microsoft 365 als jeder Administrator eines Unternehmens.

Eine gängige Technik, mit der Kriminelle M365 knacken, beschreibt Markus Seirer als Herabstufung von Benutzerlizenzen: Microsoft E5, für das sich auch sein Pharmakunde entschieden hatte, bietet ein ausgeklügeltes Identitäts- und App-Management zum Schutz vor externen Bedrohungen. Damit können bösartige Aktivitäten theoretisch erkannt und untersucht werden. „Diese Funktionen gibt es bei der E3-Lizenz größtenteils nicht. Mit der Herabstufung von Benutzerlizenzen von einer E5-Lizenz auf E3 kann der Schutz also ausgehebelt werden."

Markus Seirer, *Microsoft Licensing Professional beim CSP-Provider VENDOSOFT*

Genau das versuchen Hacker und kombinieren dieses Lizenz-Downgrade gern mit dem Missbrauch von Mailbox-Ordnerrechten. Auch das Azure Active Directory ist davor nicht gefeit: Wer sich hier Zugriff verschafft, erhält ungehinderten Zugang zu anderen Cloud-Instanzen. Allein für Microsoft 365 gibt es noch eine Reihe weiterer Beispiele. Die Sorge von IT-Leiter Dachser vor einem erneuten Cyberangriff ist also nicht unbegründet.

Bezahlbare Sicherheit

Um Computersysteme und Netzwerke vor Internetpiraterie zu schützen, müssen Unternehmen ihre Schwachstellen aufdecken, bevor es andere tun. „Als CSP-Provider raten wir unseren Kunden deshalb zu einem Cyber Security Assessment Tool", sagt Markus Seirer. Er weiß, dass IT-Verantwortliche davor zurückschrecken. Ihr Tag hat oft 14 bis 16 Stunden. Jedes Mehr an Arbeit ist eine Belastung, die als unverhältnismäßig empfunden wird. Doch die Scheu vor noch mehr Arbeit ist unbegründet. Denn CSAT, das Tool, das Seirer vorschlägt, erfordert gerade einmal zweieinhalb Stunden Arbeitsaufwand auf Seiten des Kunden. „Den Rest erledigen wir", verspricht er.

Über einen maschinellen Scan analysiert CSAT alle wichtigen Sicherheitskomponenten und leitet konkrete Handlungsempfehlungen ab, um Sicherheitslücken beim Kunden zu schließen.

Für Unternehmen mit bis zu 300 Mitarbeitern kostet das Cyber Security Assessment Tool von VENDOSOFT 1.500 Euro netto. „Das ist ein Bruchteil des wirtschaftlichen Schadens, den diese Vorsorgemaßnahme verhindern kann", appelliert der Lizenzexperte.

Das erkennt auch IT-Leiter Dachser. Das Pharmaunternehmen lässt seine Systeme nun jährlich von VENDOSOFT durchleuchten und fühlt sich gegen mögliche Cyber-Angriffe gewappnet. <

ANGELIKA MÜHLECK

VENDOSOFT
Strategische Lizenzberatung

Mehr über eine verlässliche Cyber-Sicherheit für Unternehmen unter:
www.vendosoft.de/cyber-security