Pressemitteilung

Studie in deutschen KMU:

Der deutsche Mittelstand unterschätzt die Bedrohung durch Ransomware

- 46 % der Firmen aktualisieren ihre Software nicht regelmäßig
- Mitarbeiterschulungen werden häufig vernachlässigt
- Befragung von 637 IT-Fachkräften in Deutschland, Frankreich und UK

München, 21. April 2022 – Eine neue Studie der Such- und Vergleichsplattform für Unternehmenssoftware, GetApp, analysiert, wie gut mittelständische Unternehmen in Deutschland auf Ransomware-Angriffe vorbereitet sind. Hierfür wurden 203 IT-Verantwortliche aus deutschen KMU befragt. Obwohl ein Ransomware-Angriff für die Mehrheit kritisch für die Integrität ihres Unternehmens wäre, fehlen oft noch grundlegende Sicherheitsmaßnahmen.

Highlights der Studie:

- Nur 54 % der Unternehmen aktualisieren regelmäßig ihre Software.
- 20 % haben keinen Notfall-Plan im Fall eines Ransomware-Angriffs.
- Weniger als die Hälfte (45 %) bieten ihren Angestellten regelmäßige Schulungen zum Erkennen und Melden von Ransomware-Angriffen an.
- 51 % der Unternehmen gehen davon aus, einen Ransomware-Angriff in wenigen Stunden erkennen zu können. 21 % geben an, dass sie diesen in nahezu Echtzeit erkennen würden.

Nur jedes zweite KMU nutzt Anti-Spam Software und führt regelmäßige Updates ihrer Software durch

Unter den befragten IT-Verantwortlichen gaben 76 % an, dass ein Ransomware-Angriff „etwas" bis „sehr" kritisch für die Integrität ihres Unternehmens wäre.

Zu den am häufigsten genannten Maßnahmen der befragten Unternehmen gegen Ransomware-Angriffe gehören:

- Antivirus-Software (81 %)
- Anti-Malware-Software (64 %)
- VPN (61 %)
- Software aktuell halten (54 %)
- Anti-Spam-Software (53 %)

Auch wenn ein Ransomware-Angriff kritisch für die Mehrheit der deutschen KMU ist, werden grundlegende Maßnahmen wie die Aktualisierung von Software oder die Nutzung von Anti-Spam-Software lediglich von etwas mehr als der Hälfte der Unternehmen umgesetzt.
„Deutsche KMU machen sich durch fehlende und nicht aktualisierte Sicherheitssoftware unnötig angreifbar. Unternehmen scheinen sich der Gefahr, die von Ransomware-Angriffen ausgeht, entweder nicht bewusst zu sein oder glauben, dass ihre bereits zum Einsatz kommenden Sicherheitsvorkehrungen ausreichen", so Rosalia Pavlakoudis, Content-Analystin für GetApp.

Auch wenn es um unternehmensweite Notfallpläne gibt, hat die Befragung gezeigt, dass es hier noch Lücken unter den deutschen KMU gibt. 20 % der IT-Verantwortlichen gaben an, keinen Notfallplan für den Fall eines Ransomware-Angriffs zu haben und 7 % waren sich nicht sicher.

Mitarbeiterschulungen zur Minimierung des Sicherheitsrisikos

Unwissenheit und Unachtsamkeit von Mitarbeitern kann Malware ungewollt Zugang zum Unternehmen ermöglichen. Dieses Sicherheitsrisiko kann von Unternehmen durch regelmäßige Mitarbeiterschulungen deutlich reduziert werden.

Weniger als die Hälfte der Befragten (45 %) gaben an, dass sie ihre Angestellten regelmäßig dazu schulen, wie sie potenzielle Ransomware-Angriffe erkennen und melden. Ein Drittel führte ein bis zwei Schulungen durch. 19 % berichten, dass noch keine Schulungen angeboten werden, sie aber geplant seien, und 2 % bieten keine Schulungen an und haben es auch nicht vor.

In Großbritannien dagegen werden mehr Mitarbeiter geschult. So gaben nur 6 % an, dass sie noch keine Schulungen anbieten, aber es vorhaben und 3 %, dass keine Schulungen geplant sind. Frankreich schließt in diesem Punkt am schlechtesten ab: 20 % der KMU führen noch keine Schulungen durch, aber haben es vor, während 6 % es sich nicht vornehmen.

Die wichtige Rolle der Angestellten wird auch in den Antworten der IT-Spezialisten auf die Frage, ob sie ihr Unternehmen für ausreichend geschützt einschätzen, deutlich: „*Wenn unsere Mitarbeiter noch besser geschult werden, bin ich sehr zuversichtlich, dass mein Unternehmen sehr gut geschützt ist*." Ein weiterer Teilnehmer sagte aus, dass mögliche Schwachstellen Mitarbeiter und Unaufmerksamkeiten seien.

Hohe Zuversicht, den Ransomware-Angriff schnell entdecken zu können

Trotz häufig fehlender Maßnahmen, denken nur 2 % der Befragten, dass ihr Unternehmen Wochen benötigen würde, um einen Ransomware-Angriff zu erkennen. 24 % denken, dafür einen Tag bis wenige Tage zu benötigen, während die Hälfte der Teilnehmer davon ausgeht, einen Ransomware-Angriff bereits innerhalb von Stunden zu erkennen. 21 % denken, dass ihr Unternehmen einen Angriff nahezu in Echtzeit bemerken würden.

Außerdem gaben 66 % der Befragten an, dass sie auf den Fall vorbereitet sind, dass ein Angriff am Wochenende oder an Feiertagen geschieht.

In Großbritannien gaben sogar 75 % der Unternehmen an, auf einen Angriff am Wochenende vorbereitet zu sein, während es in Frankreich nur 59 % sind.

Methodik der Umfrage

Um die Daten für diese Studie zu erheben, hat GetApp im März 2022 eine Online-Umfrage durchgeführt. Als Teilnehmer wurden insgesamt 637 IT-Fachkräfte zum Thema Ransomware in ihrem Unternehmen befragt, 203 davon in Deutschland, 200 in Frankreich und 234 in der UK. Weitere Auswahlkriterien waren:

- Wohnsitz in Deutschland, Frankreich oder UK.
- Über 18 Jahre alt.
- Beruf: IT-Spezialist, Manager/Entscheidungsträger in IT-/Cybersecurity-Abteilungen.
- Aktuell in einem Unternehmen mit 2 bis 250 Mitarbeitern beschäftigt.

Über GetApp

GetApp ist eine Such- und Vergleichsportal, die kleinen und mittelständischen Unternehmen hilft, die richtige Softwareauswahl zu treffen. GetApp unterstützt KMU mit maßgeschneiderten, datengesteuerten Empfehlungen und Erkenntnissen, die sie für ihre Software-Kaufentscheidungen benötigen. Weitere Informationen finden Sie unter www.getapp.de.