

Pressemitteilung

Wie COVID-19 die IT-Sicherheit in KMU beeinträchtigt

IT-Entscheider zur Lage in deutschen Unternehmen

München, 08.06.2021 – Capterra, die führende Bewertungsplattform für Unternehmenssoftware, veröffentlicht eine Studie zum Stand der IT-Sicherheit in deutschen KMU. Dazu wurden IT-Entscheider aus kleinen und mittelständischen Unternehmen befragt, um Einblicke in die derzeit größten IT-Risiken, die Entwicklung der Angriffe während der Krise und den allgemeinen Sicherheitsstandard zu geben.

Einige Highlights der Studie:

- 36 % nutzen bereits künstliche Intelligenz für ihre IT-Sicherheit und weitere 44 % sind an der Technologie interessiert.
- Die Nutzung biometrischer Sicherheitsmaßnahmen ist im letzten Jahr um 30 % gestiegen.
- 47 % der Unternehmen investierten aufgrund von COVID-19 mehr in die IT-Sicherheit.
- Die meistgenannten Bedrohungen sind E-Mail-Phishing, Leichtsinns der Endnutzer und gezielte Hackerangriffe.

Fast jedes zweite Unternehmen fiel bereits einer Cyberattacke zum Opfer

44 % der Unternehmen waren bereits Opfer eines Cyberangriffs; unentdeckte Attacken sind darin nicht enthalten. Die Auswirkungen sind oft fatal. Ein betroffenes Unternehmen teilte mit: "Wir konnten nicht mehr auf unsere PCs zugreifen und haben 100.000 Euro Verlust gemacht".

E-Mail Phishing ist die meistgenannte Bedrohung: 77 % der Unternehmen haben bereits eine Phishing-E-Mail erhalten. Von diesen Unternehmen geben 44 % an, dass sie während der Krise mehr Phishing-E-Mails als gewöhnlich erhalten.

Die Krise hat dazu geführt, dass viele Sicherheitsanwendungen erstmalig in KMU eingesetzt wurden. Vor allem VPN Software sah einen großen Anstieg. Auch vorher wenig genutzte Anwendungen wie Endpoint Protection Platform (EPP) und Endpoint Detection and Response (EDR) wurden während COVID-19 angeschafft.

Die künstliche Intelligenz ist die Zukunft der IT-Sicherheit

80 % der Unternehmen setzen KI bereits ein oder sind an der Technologie interessiert. Cyberangriffe treten nicht nur häufiger auf, sondern werden auch immer komplexer. Künstliche Intelligenz kann Anomalien schneller erkennen, Risiken und Risikobereiche vorhersagen und den Cybersicherheitsplan robuster gestalten.

Befragt wurden 202 Voll- oder Teilzeitbeschäftigte aus kleinen und mittelständischen Unternehmen (mit 2-250 Mitarbeitern), die für Entscheidungen über IT-Richtlinien in Ihrem Unternehmen teils oder voll verantwortlich sind.

Über Capterra

Capterra hilft Unternehmen weltweit, die richtige Software für ihre Anforderungen zu finden. 1999 gegründet, bietet Capterra mit seiner globalen Produktpräsenz, verifizierten Nutzerbewertungen, unabhängigen Testberichten und maßgeschneiderten Vergleichstools jeden Monat mehr als fünf Millionen Käufern Zuversicht bei der Softwareauswahl. Weitere Informationen unter [capterra.com.de](https://capterra.com/de).