Studie “Cybersicherheit in klein- und mittelständischen Unternehmen” - Informationsstand im Mittelstand zur Cyberkriminalität immer noch lückenhaft

● Über 90 % der mittelständischen Unternehmen haben Erfahrung mit Cyber-Vorfällen gemacht ● Fast ein Drittel der Unternehmen nutzt kein Datenbackup ● Risikofaktor “Mensch” findet kaum Beachtung: 75 % schulen ihre Mitarbeiter nicht

Am 27. Juni 2018 jährte sich der Cyberangriff der Ransomware (Erpressungssoftware) “NotPetya”, die über MS-Office Dokumente erfolgte und international Schäden in Millionenhöhe angerichtet hatte. Kein Einzelfall. Mehrere Studien belegen, dass das Risiko „Cyber-Attacke“ in den letzten Jahren signifikant gestiegen ist. Obwohl vor allem klein- und mittelständische Unternehmen besonders häufig von Hacker-Angriffen bedroht und betroffen sind, zeigen die Ergebnisse einer aktuellen Studie von CyberDirekt nun auf, dass fast alle der befragten Unternehmen immer noch Nachholbedarf beim Thema IT-Sicherheit haben und die Gefahren durch Cyberkriminalität unterschätzen.

Die aktuelle Studie “Cybersicherheit in klein- und mittelständischen Unternehmen”, welche vom Berliner Unternehmen CyberDirekt und dem unabhängigen Marktforschungsinstitut INNOFACT AG durchgeführt wurde, hat den Informationsstand in klein- und mittelständischen Unternehmen (bis 20 Mitarbeiter) untersucht und konnte aufzeigen, dass trotz steigenden Risikos – über 90 % der Befragten haben in den letzten zwei Jahren bereits Erfahrung mit Cyber-Vorfällen gemacht –, nur 30 % der Unternehmer eine tatsächliche Bedrohung wahrnehmen.

Deutlich wurde zudem, dass immer noch nicht alle Unternehmen Basis-Maßnahmen zur Sicherung ihrer Daten umsetzen. So verfügen knapp ein Drittel der Unternehmen über kein Datenbackup. Gerade vor dem Hintergrund von Angriffen durch Ransomware oder Verschlüsselungstrojaner birgt dies eine große Gefahr, Daten unwiderruflich zu verlieren. Die häufigsten Maßnahmen zur Absicherung gegen Cyber-Angriffe sind Anti-Viren-Software (84 %), Firewalls (80 %) und die Verwendung von starken Passwörtern (78 %).

Vor allem bei der Frage nach der Gefahrenquelle offenbart sich zudem, dass der Risikofaktor “Mensch” im Sicherheitsdenken der befragten Unternehmen weiterhin unterschätzt wird. 75 % der Unternehmer nutzen keine Schulungs- oder Weiterbildungsangebote zu Themen wie IT-Sicherheit und Cyberkriminalität für ihre Mitarbeiter. Die Risiken aus der Kommunikation mittels Messenger-Diensten (z.B. WhatsApp) unter Kollegen oder Social-Media Nutzung am Arbeitsplatz wird nur von ca. 20% der Unternehmen als Gefahrenquelle wahrgenommen. In drei Viertel aller kleinen Unternehmen gibt es keine abgestuften Nutzerrechte, d.h. alle Mitarbeiter haben Zugriff auf sensible Daten. Dabei erfolgen die meisten Attacken auf kleine und mittlere Unternehmen über Phishing, Social Engineering und beispielsweise als Bewerbungen getarnte Email-Anhänge.

Dass KMUs im besonderen Maße von Cyberkriminalität betroffen sind, davon ist auch Hanno Pingsmann, Geschäftsführer von CyberDirekt überzeugt: “Durch Attacken von Cyberkriminellen sind besonders zwei Gruppen betroffen – kleine und mittelständische Unternehmen, welche sich aufgrund von Größe und Budgetrestriktionen nicht ausreichend vor Angriffen schützen können und Unternehmen, welche mit einer hohen Zahl von personenbezogenen Daten arbeiten und in deren Alltag Kundenvertrauen und Reputation eine große Rolle spielen.”

Datensicherheit und Datenschutz sind folglich gerade in kleinen und mittelständischen Unternehmen essentiell. Denn selbst ungezielte Angriffe aus dem Netz führen im Extremfall zum Ausfall der gesamten EDV-Infrastruktur mit katastrophalen finanziellen Folgen für die Unternehmen. Neben der Unterbrechung des Betriebs und den Kosten für die Bereinigung und Wiederherstellung der Systeme sind die Unternehmen dem unter der DSGVO verschärften Haftungsrisiko ausgesetzt, welches sich aus einer Datenschutzverletzung ergibt. Folglich verwundert es nicht, dass sich über die Hälfte der befragten Unternehmer in einem Notfall vor allem eine Kostenübernahme für die Wiederherstellung der Systeme und einen Haftpflichtschutz für Datenschutzverletzungen wünschen.

Eine Versicherung gegen Cyber-Attacken kann hier eine Möglichkeit sein, um sich gegen Schäden abzusichern und im akuten Fall auf eine effektive Unterstützung zurückgreifen zu können. Dabei ist es wichtig die Angebote der Versicherer auf die individuelle Unternehmensstruktur hin zu prüfen, um so das optimale Angebot zu ermitteln. Mit CyberDirekt, steht kleinen und mittleren Unternehmen (KMU) eine digitale Plattform für den Abschluss von Cyber-Versicherungen zur Verfügung, über die Versicherungen auf die individuelle Bedürfnisse hin geprüft werden können. Die über CyberDirekt abschließbaren Versicherungen bieten eine Absicherung gegen die Folgen eines Cyber-Angriffs sowie kostenfreie Online-Schulungen für Mitarbeiter, um die Risiken bereits umfassend präventiv zu minimieren und im Ernstfall vorbereitet zu sein. Das Angebot richtet sich speziell an Unternehmen und Freiberufler mit einem Umsatz von bis zu 10 Millionen Euro.

Zur Studie
Mit dem Projekt “Cybersicherheit in KMU” wurde der Informationsstand zur Cyberkriminalität in deutschen Unternehmen beleuchtet, die Änderung der Gewohnheiten aufgrund von Sicherheitsbedenken aufzeigt und den Grad der Besorgnis sowie die wirkliche Wahrnehmung vor einzelnen Formen der Cyberkriminalität aufgedeckt. Die Ergebnisse der Studie bilden dabei unter anderem die Grundlage um effektive Handlungsanweisungen zur Risikominimierung zu definieren.

KONTAKT
Nadine Brunner | Account Director | Clarity PR
M: +49 172 1 888 203