



Berlin, 3. Mai 2021

## **AG „IT-Sicherheit\_Cybercrime“ gestartet – Bundesinnungsverband des Gebäudereiniger-Handwerks (BIV) entwickelt Handlungsempfehlungen für Unternehmen**

**Ob Ransomware oder Phishing-Attacken – nicht nur die Zahl der betroffenen Computer, Smartphones und digitalen Netzwerke steigt, sondern auch die Professionalität der Täter und die Zahl der Attacken – auch auf Unternehmen. Der Schaden kann dabei in die Millionen gehen. Eine viel beachtete Umfrage des Spezialversicherers [Hiscox](#) kommt aktuell zu dem Ergebnis, dass fast jedes zweite befragte Unternehmen in Deutschland mindestens einmal von einer Cyberattacke betroffen war. Darunter sind in jüngster Zeit auch zunehmend Betriebe des beschäftigungsstärksten deutschen Handwerks. „Der Handlungsbedarf ist groß“, so Bundesinnungsmeister Thomas Dietrich. „Die Frage ist nicht, ob eine Cyberattacke kommt, sondern wann“. Daher hat der Bundesinnungsverband des Gebäudereiniger-Handwerks (BIV) die neue Arbeitsgemeinschaft ins Leben gerufen.**

In der AG „IT-Sicherheit\_Cybercrime“ diskutieren 20 Expertinnen und Experten aus den BIV-Mitgliedsunternehmen und erarbeiten gemeinsam Lösungsvorschläge: Wo liegen technisch die größten Angriffsflächen in Unternehmen? Welche Warnzeichen können Beschäftigte beachten? Welche Hard- und Softwarelösungen bieten Schutz?

Von hoher Aktualität ist die Thematik auch aufgrund der Pandemie. Da deutlich mehr Beschäftigte im Homeoffice arbeiten, vergrößert sich die Angriffsfläche, etwa in Form von Phishing-Attacken. In den kommenden Wochen wird die Arbeitsgemeinschaft eine erste Handlungsempfehlung erarbeiten, in der die Prävention im Zentrum steht.

„Unsere Aufgabe ist es, gerade unsere oft kleinen und mittelständischen Unternehmen von diesem dramatisch zunehmenden Problembereich zu überzeugen“, so Bundesinnungsmeister Thomas Dietrich. „Jedes Unternehmen sollte die Gefahren durch Cyberkriminalität kennen und sich personell und technisch vorbereiten. Hier machen wir als BIV für alle Mitgliedsunternehmen praktikable Angebote.“

Eine zweite Handlungsempfehlung der AG „IT-Sicherheit\_Cybercrime“ soll Unternehmen aufklären, welche Akut-Maßnahmen im Fall einer erfolgten Attacke zu ergreifen sind. Die Arbeit der Arbeitsgemeinschaft soll bis Sommer abgeschlossen sein.