zvdh-kompakt

43/2018

IT-Sicherheit

Köln, 9. November 2018

IT-Sicherheit ist auch für das Dachdecker-Handwerk ein wichtiges Thema, das leider im Alltag oft zu kurz kommt. Der Informationsbedarf, aber auch die Unsicherheit ist hoch, und das nicht erst seit der Datenschutzgrundverordnung. Dies führt auch zu einem Stillstand bei eigentlich notwendigen Digitalisierungsprozessen. Studien belegen, dass Cyber-Sicherheit immer noch eines der größten Hemmnisse für Handwerksbetriebe darstellt, den Schritt in die Digitalisierung zu wagen. Zum Teil sind die Ängste nicht ganz unberechtigt, denn durch die rapide zunehmende Vernetzung von Systemen werden auch Handwerksunternehmen zu einem begehrten Ziel von Hackerangriffen, Schadsoftware, Phishing und anderen Cyber-Attacken. Cyber-Sicherheit wird vor diesem Hintergrund zu einer wesentlichen Voraussetzung für eine erfolgreiche Digitalisierung.

Allianz für Cybersicherheit

Die Allianz für Cyber-Sicherheit ist eine Initiative, die in Unternehmen das Know-how zum Schutz vor Cyber-Angriffen stärkt. Sie bietet als Plattform zur Kooperation mit Wirtschaft, Behörden, Forschung und Wissenschaft sowie anderen Institutionen ein breites Informationsangebot rund um Cyber-Sicherheit. Im besonderen Fokus der Initiative stehen kleine und mittelständische Unternehmen. Das Handwerk ist über den Zentralverband des Deutschen Handwerks (ZDH) im Beirat der Allianz vertreten. Als Betrieb kann man kostenlos Teilnehmer der Initiative werden; die Angebote der Allianz für Cyber-Sicherheit sind hier abrufbar: www.allianz-fuer-cybersicherheit.de. Auf dieser Seite gibt es auch eine Meldestelle für Hackerangriffe sowie eine Liste mit Kontaktdaten der für Cyberkriminalität zuständigen Stellen des Bundeskriminalamtes sowie aller Landeskriminalämter.

Speichern in der Cloud

Daten, Notizen, Fotos, Kontakte: Vieles wird bereits in der Cloud gelagert. Cloud bedeutet die Bereitstellung von IT-Infrastrukturen wie beispielsweise Speicherplatz über das Internet. Zu Beginn der Cloud-Nutzung ist es je nach Dienst möglich, die Standardeinstellungen zu ändern; dies sollte man unbedingt vornehmen. Denn oft ist es so, dass nicht nur der Cloud-Betreiber Einblick in die Daten bekommt, sondern auch andere Internet-User, etwa wenn Dokumente mit Cloud-Anwendungen verfasst werden. Geprüft sollten daher auch die Allgemeinen Geschäftsbedingungen. Eine große Rolle spielt, wo die Server stehen und die Daten verarbeitet werden. Je nach Land gelten ein anderes Datenschutzniveau und eine andere Rechtslage. Sensible Daten sollten auf jeden Fall nur verschlüsselt in die Cloud gestellt werden. Dazu gibt es verschiedene Verschlüsselungsprogramme. Der Cloudbetreiber darf keinen Schlüssel zum Entsperren der Dokumente besitzen. Experten raten übrigens, wirklich „lebensnotwendige“ Dateien nicht im Web zu speichern, sondern davon Sicherheitskopien (Backups) auf externen Festplatten oder USB-Sticks zu machen und diese an unterschiedlichen Standorten aufzubewahren. Natürlich müssen diese regelmäßig aktualisiert und auch verschlüsselt werden.

Sichere Cloud

Ganz aktuell hat Google für die Google-Cloud-Services „G Suite“ und „Google Cloud Platform“ mit dem C5-Testat an allen Standorten weltweit die Sicherheitsanforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) erfüllt. Im C5-Katalog hat das BSI Anforderungen zusammengefasst, die Cloud-Anbieter erfüllen sollten, um ein Mindestmaß an Sicherheit ihrer Cloud-Dienste zu gewährleisten. Der C5-Katalog ist ein Standard, der prüfbare Anforderungen beinhaltet, aber nicht vorschreibt, durch welche Maßnahmen diese zu erfüllen sind. Der Anforderungskatalog steht auf der Webseite des BSI zum Download zur Verfügung. https://www.bsi.bund.de

Herausgeber: Zentralverband des Deutschen Dachdeckerhandwerks e.V., Fritz-Reuter-Straße 1, 50968 Köln
☎ 0221-398038-0 0221-398038-99 E-Mail zvdh@dachdecker.de // Internet www.dachdecker.de
https://facebook.com/DachdeckerDeinBeruf Verantwortlich: Claudia Büttner