



Gegen Hackerangriffe sollten sensible Daten nur verschlüsselt in der Cloud gespeichert werden.

Sicherheit geht vor

Digitalisierung: IT-Sicherheit ist auch für das Dachdeckerhandwerk ein wichtiges Thema, das leider im Alltag oft zu kurz kommt. Informationsbedarf und Unsicherheit sind hoch, und das nicht erst seit der Datenschutz-Grundverordnung. Dies führt auch zu einem Stillstand bei eigentlich notwendigen Digitalisierungsprozessen. Teil 3 unserer Digitalisierungsreihe informiert, wie sich Dachdeckerbetriebe schützen können.

Claudia Büttner

Studien belegen, dass Cybersicherheit 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 Cyberattacken. Knapp 70% der Unternehmen und Institutionen in Deutschland sind in den Jahren 2016 und 2017 Opfer von Cyberangriffen geworden. In knapp der Hälfte der Fälle waren die Angreifer erfolgreich und konnten sich zum Beispiel Zugang zu IT-Systemen verschaffen, die Funktionsweise von IT-Systemen beeinflussen oder Internetauftritte von Firmen manipulieren. Jeder zweite erfolgreiche Angriff führte dabei zu Produktions- bzw. Betriebsausfällen. Hinzu kamen häufig noch Kosten für die Aufklärung der Vorfälle und die Wiederherstellung der IT-Systeme sowie Reputationsschäden. Dies geht aus der Cyber-Sicherheits-Umfrage 2017 hervor, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen der Allianz für Cybersicherheit durchgeführt hat und an der circa 900 -Unternehmen und Institutionen teilnahmen. Cybersicherheit wird vor diesem Hintergrund zu einer wesentlichen Voraussetzung für eine erfolgreiche Digitalisierung.

Allianz für Cybersicherheit

Um sich in der Fülle der Informationen zurechtzufinden und vor allem auch seriöse Auskunft zu erhalten, kann die Teilnahme an der Allianz für Cybersicherheit sinnvoll sein. Diese Initiative will das Know-how in Unternehmen zum Schutz vor Cyberangriffen stärken und bietet ein breites Informationsangebot rund um Cybersicherheit. 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 Cybersicherheit 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 Bundeskriminalamts sowie aller Landeskriminalämter. Konkret wird folgendes angeboten:

1. aktuelle Warnmeldungen, Lageberichte zur Cybersicherheit in Deutschland, Lösungshinweise und praktische Anleitungen
2. Wissens- und Erfahrungsaustausch: Thematische Cybersicherheitstage, Erfahrungs- und Expertenkreise
3. Ausbau von Sicherheitskompetenz: Schulungen und Workshops, Analysen und Erstberatung, Penetrationstests

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 Internetuser, 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 Cloud-Betreiber darf keinen Schlüssel zum Entsperren der Dokumente besitzen. Experten raten übrigens, wirklich „lebensnotwendige“ Dateien nicht im Web zu speichern, sondern Sicherheitskopien (Backups) davon auf externen Festplatten oder USB-Sticks zu machen und diese an unterschiedlichen Standorten aufzubewahren. Natürlich müssen diese regelmäßig aktualisiert und auch verschlüsselt werden.

Members only

Im internen Bereich finden Innungsmitglieder wertvolle Hinweise, Checklisten und Textbausteine rund um die Neuerungen durch die Datenschutz-Grundverordnung. Die Inhalte werden regelmäßig aktualisiert, die letzten Einträge befassen sich mit Fragen zu Whatsapp und Facebook-Fanseiten. Einfach Einloggen unter <https://member.dachdecker.de> und auf die Kachel „Leitfaden DSGVO“ klicken.

A - Einführung

Um den Datenschutz in allen Mitgliedsbetrieben der Innung zu gewährleisten, gelten ab dem 25. Mai 2018 in allen EU-Ländern in Deutschland betreffend die Veränderungen in einer Linie formale Vorschriften. Die folgenden „Wichtigsten Verbote“ beschreiben sich auf die wesentlichen Änderungen für Dachdeckerbetriebe. Durch Klick auf die jeweilige Leitfaden wird jeder Punkt ausführlich erläutert. Wir haben unterstehend die wichtigsten Regelungen so strukturiert, dass gewalt das Thema anstimm, dass für Ihren Betrieb relevant ist. Dort finden Sie auch die jeweils passenden Muster und Vorlagen aufgeführt und können dort direkt heruntergeladen werden. Ein rascher Überblick verschafft der Online-

- ZVDH-Merkblatt als PDF zum Download
- ZdH-Leitfaden mit Musterunterlagen als PDF zum Download
- Weg zur DSGVO - Selbstinspektion

B - Das ist zu tun: Die wichtigsten Schritte

Unter jeder der aufgeführten Schritte finden Sie Musterformulare, die Sie je nach Bedarf auf Ihrer Website einbauen können um sicher zu sein Ihre Maßnahmen umsetzen können.

1. Datenschutzerklärung anpassen - Webseite
2. Kunden informieren
3. Dokumentationspflicht / Verarbeitungsverzeichnis
4. Externe Dienstleister / Auftragsverarbeitung
5. Mitarbeiter informieren
6. Datenschutzbeauftragter

C - FAQ Die häufigsten Fragen:

1. Wann ist eine Datenutzung ohne Einwilligung des Betroffenen zulässig?
2. Wie muss ich Kunden und Mitarbeiter über die von Ihnen erhobenen Daten informieren? Wie?
3. Welchen Umfang hat die neue Dokumentationspflicht?
4. Welche Folgen drohen bei Verstößen?
5. Wann ist ein Datenschutzbeauftragter zu benennen?
6. Welche Auswirkungen hat das ZGDH-Urteil zu den Fanseiten bei Facebook? **UPDATE**
7. Welche Auswirkungen hat die DSGVO auf die Nutzung von WhatsApp?

D - Übersicht aller Muster und Vorlagen:

- Auftragsverarbeitung_Google_DSGVO_2018.pdf
- Auftragsverarbeitung_Hinweis_Betriebe.docx
- Informationspflicht_Arbeits_Schwerung_3.docx

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: www.bsi.bund.de. //

Autorin

Claudia Büttner ist
Pressesprecherin des ZVDH.

