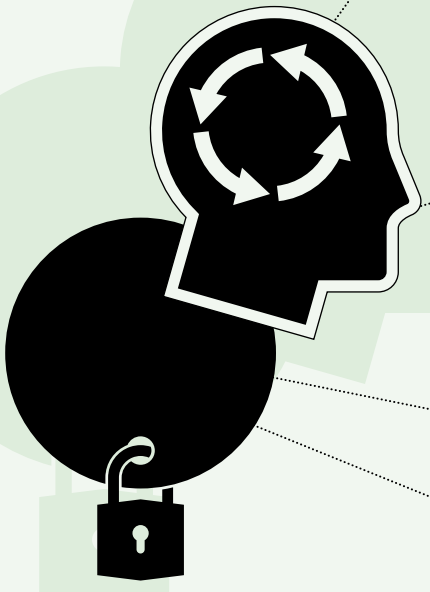
TIPPS & TRICKS

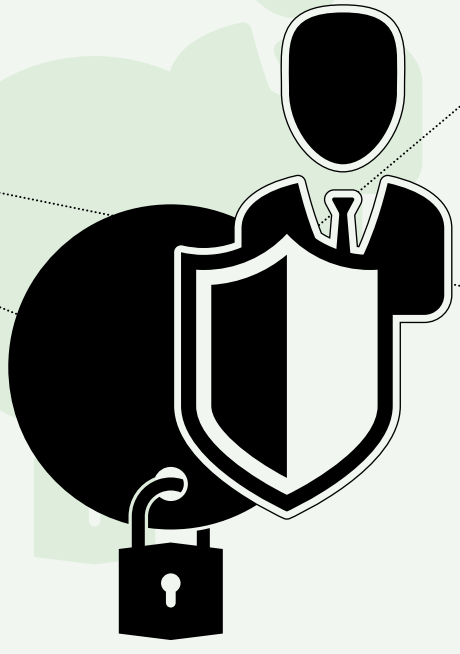
VOLLE DECKUNG

Alle reden von Digitalisierung, aber denkt auch jemand an die Sicherheit? Immer öfter berichten Kunden von Cyberangriffen, durch die Jobdaten verloren gehen oder gar die Produktion ausfällt. Die Ausrede „Wir sind zu uninteressant für einen Angriff“ zählt dabei nicht: Jeder ist ein potenzielles Opfer – wenn er sich nicht an diese einfachen Regeln hält.



FIREWALL IM KOPF EINREISSEN

Gerade kleine Druckereien wiegen sich in falscher Sicherheit, wenn sie denken, bei ihnen gebe es nichts zu holen. Personenbezogene Daten wie Bankverbindungen oder Adressinformationen sind immer interessant für Angreifer – und davon hat jede Druckerei genug. Zudem erfolgen die meisten Angriffe automatisiert und suchen sich das schwächste Glied in der Wertschöpfungskette. Die Mitarbeiter zu sensibilisieren ist daher das oberste Gebot und der erste Schritt in Richtung Datensicherheit.



DEN HUT AUFSETZEN

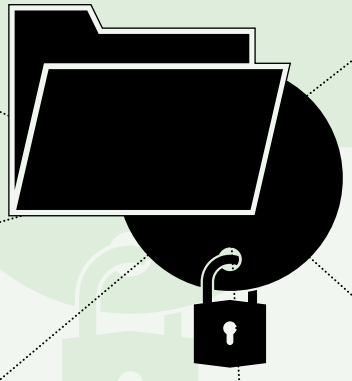
Gibt es keinen Verantwortlichen, verlaufen Maßnahmen im Sande. Legen Sie deshalb einen Sicherheitsbeauftragten fest. Er dokumentiert, welche Geräte und Software zu welchem Zweck und von welchen Mitarbeitern verwendet werden. Davon leitet er Sicherheitsrichtlinien und Maßnahmen ab, wie sich Risiken vermeiden und gesetzliche sowie vertragliche Vorgaben einhalten lassen, und dokumentiert sie. Wenn die Geschäftsführung dann auch noch ihr Engagement in Sachen Datensicherheit vorlebt, schließen sich die Lücken für Angreifer.

Das White Paper von Heidelberg zur IT-Sicherheit in Druckereien:

www.heidelberg.com/IT-Sicherheit-Whitepaper

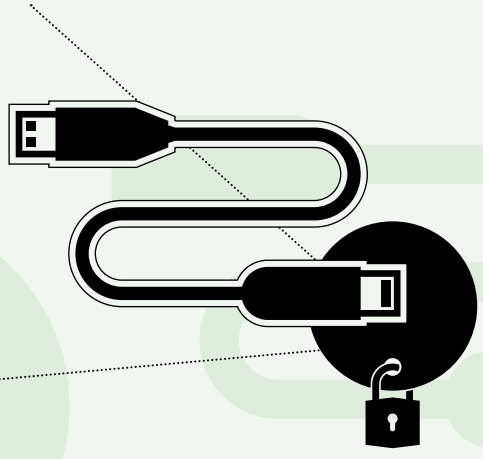
ZWEIGLEISIG FAHREN

Sensible Daten gehören verschlüsselt. Dieser simple Leitsatz gilt sowohl für die Ablage als auch für den Versand von Informationen. Und für den Fall des Verlustes gilt: kein Back-up, kein Mitleid. Tägliche Sicherungskopien auf externen Speichermedien schützen vor Datenverlust, etwa bei einer Infektion des Firmennetzes mit Ransomware.



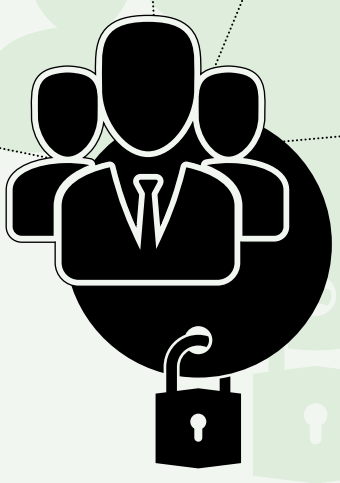
DAS RICHTIGE MATERIAL VERWENDEN

Veraltete Software bietet Angreifern viele Ansatzpunkte. Das gilt auch für Programme, die gar nicht genutzt werden. Etwa Anwendungen, die der Hersteller installiert hat. Unnötige Software sollten Sie daher entfernen, benötigte Programme immer mit Updates auf dem neuesten Stand halten. Benutzen Sie zudem für jede Anwendung und jedes Gerät unterschiedliche Passwörter. Sie sollten mindestens acht Zeichen lang sein, aus Ziffern, Buchstaben und Sonderzeichen bestehen sowie in regelmäßigen Abständen erneuert werden. Tabu sind Namen, Geburtstage oder Zahlenfolgen wie 123456. Ein aktueller Virenschutz sollte für alle Geräte Standard sein, auch für mobile Rechner, die eventuell im Home Office der Mitarbeiter genutzt werden.



DER VERSUCHUNG WIDERSTEHEN

Komfortable Online-Dienste wie Dropbox stellen neben dem Sicherheitsrisiko auch aus Compliance-Gründen eine Gefahr dar. So ist es selten ersichtlich, in welchem Rechenzentrum beziehungsweise Rechtsgebiet die Dateien landen. Viele Druckereien verwenden zudem immer noch das Übertragungsprotokoll FTP. Doch Einfachheit hat ihren Preis: FTP verschickt Daten unverschlüsselt, Angreifer können unter Umständen Passwörter abgreifen und für Attacken nutzen. Daher zumindest erweiterte Varianten wie SFTP oder FTPS nutzen, die mehr Sicherheit beim Datenversand bieten.



SEINE ROLLE SPIELEN

In vielen Fällen treten Mitarbeiter durch unbedachtes Verhalten wie das Öffnen von Anhängen in dubiosen E-Mails eine Lawine los, indem sie Viren, Trojaner oder – wie in jüngster Vergangenheit weltweit mit „WannaCry“ geschehen – sogenannte Ransomware ins Unternehmensnetzwerk schleusen. Um das Risiko zu minimieren, sollten sie grundsätzlich nur Zugriffsrechte auf solche Daten, Netzwerke und Software erhalten, die sie für die Arbeit brauchen. Administratorrechte tragen ihren Namen schließlich nicht umsonst: Sie sind Administratoren vorbehalten. Das verhindert uneingeschränkten Zugriff von Schadcode auf das gesamte System.

ZAHLEN UND FAKTEN

53 Prozent aller Firmen in Deutschland wurden bereits Opfer von Sabotage, Spionage oder Datendiebstahl.
Quelle: Studie des Bundesverfassungsschutzes

Die Ransomware „WannaCry“ legte im Mai innerhalb weniger Stunden Hunderttausende Computersysteme in mehr als 150 Ländern lahm. Die Angreifer nutzten eine Sicherheitslücke in Microsofts Betriebssystem Windows. Betroffen waren nur Geräte, auf denen aktuelle Updates fehlten.
Quelle: Süddeutsche Zeitung

Im vergangenen Jahr betrug der **Lösegelderlös** von Kriminellen durch Ransomware mehr als 1 Milliarde Dollar. Die Software für Angriffe dieser Art ist im Internet bereits für 28 Dollar erhältlich.
Quelle: Frankfurter Allgemeine Zeitung