# DATENSICHERHEIT:
# DAS SIND DIE HÄUFIGSTEN FEHLER IM HANDEL

Die Digitalisierung hat schon lange Einzug in den Handel gehalten. Bestellung, Lieferung und Bezahlung laufen bei vielen Unternehmen online ab und vereinfachen nicht nur die Logistik, sondern auch die Kundenkommunikation. Welche Risiken das für den Datenschutz bedeutet und was Einzelhändler für mehr Datensicherheit tun können, erklärt Expertin Marie Schneider.

Cyberkriminalität und Datenklau sind in den vergangenen Jahren zu einem immer größeren Thema im Online-Handel geworden. Ob E-Mail-Adressen, Zahlungs- oder Zugangsinformationen – sie erweisen sich als wertvolle und oftmals leider sehr einfache Beute für Hacker.

**"Händler unterschätzen die Gefahren im Netz"**
Der Grund: Händler unterschätzen die Gefahren im Netz und versäumen es, ganzheitliche Schutzmaßnahmen einzuführen. Diese sollten sich nämlich nicht nur auf Sicherheitssysteme beschränken, sondern auch den richtigen Umgang mit Firmendaten beinhalten. Denn menschliche Fehler sind eine der Hauptursachen für Verstöße gegen die Datensicherheit.

**Datendiebstahl: Besser vermeiden.**

Doch wie kommen diese Sicherheitspannen zustande und welche Möglichkeiten haben Online-Händler, um die Gefahren einzudämmen?

**E-Mails: Böse Phishing-Fallen**
Eine nach wie vor häufige Methode von Betrügern ist der Versuch, mittels gefälschter Webseiten, E-Mails und Kurznachrichten an vertrauliche Informationen eines Unternehmens zu gelangen. E-Mails stellen dabei die größte Angriffsfläche dar, weshalb eine zielgerichtete Schulung der Mitarbeiter von enormer Bedeutung ist, um Datenklau zu verhindern.

Damit sollen die Angestellten nicht nur vom Klick auf den gefährlichen Link abgehalten werden, sondern auch verstehen, wie Social-Engineering-Angriffe funktionieren. Zudem sind regelmäßige Simulationstests zu empfehlen, in denen die Effektivität der Schulung sowie die Einhaltung der Sicherheitsrichtlinien nachgeprüft wird.

**Falsche E-Mail-Empfänger begünstigen Datenklau**
Dass das Personal eine geschäftliche E-Mail dem falschen Adressaten zusendet, passiert in der Realität immer noch häufiger als gedacht. Es handelt sich dabei sogar um die vierthäufigste Sicherheitspanne, die Datenklau begünstigt.

Und dass, obwohl das Schreiben und Versenden von Mails in den allermeisten Unternehmen zum Tagesgeschäft gehört und das zentrale Kommunikationsmittel darstellt. Vor allem in der Gesundheitsbranche kommt es häufig dazu, dass Mitteilungen aus dem Labor an den falschen Empfänger verschickt werden, was nicht selten zu unschönen Missverständnissen und Imageschäden führt.

Daher tun Händler gut daran, alle Nachrichten, die sensible Daten enthalten, zu verschlüsseln. Um das Risiko zu minimieren, dass der Absender eine falsche E-Mail-Adresse angibt, können Popup-Fenster ihn daran erinnern, diese vor dem Abschicken nochmals zu kontrollieren.

Eine Data Loss Prävention-Lösung sowie spezielle Sicherheitssoftware können ebenfalls dazu beitragen, vertrauliche Informationen zu identifizieren und Mitarbeiter an deren Verbreitung außerhalb des Firmennetzwerkes zu hindern.

**Sicherheitslücken bei externen Zugriffen**
Immer mehr Betriebe ermöglichen ihren Angestellten flexible Arbeitszeiten sowie die Option zum Homeoffice. Damit steigt die Gefahr, dass nicht autorisierte Benutzer auf sensible Daten zugreifen können. Möglicherweise befindet sich auch Malware im genutzten Netzwerk und gelangt beim Arbeiten auf den Firmenlaptop.

Zudem finden Online-Speicher zunehmend Verwendung, wenn die Datenmengen für den Betriebsserver zu groß werden. Insbesondere bei komplexen ERP-Systemen kommen immer häufiger Cloud-Lösungen zum Einsatz. So lassen sich unternehmerische Prozesse flexibel und unkompliziert steuern.

**Sicherheitskontrollen auf mobilen Endgeräten**
Bei allen Vorteilen, von denen Händler dank der digitalen Vernetzung profitieren, sollten sie dabei die Risiken der virtuellen Welt nicht aus den Augen verlieren. Viele Firmen sind sehr gut gerüstet, was die Sicherheit der eigenen internen IT angeht.

Doch bei den Schutzmaßnahmen für externe Kommunikationswege und digitale Speicherorte sind die meisten Unternehmen noch zu nachlässig. Es empfiehlt sich, auf allen (auch mobilen) Arbeitsgeräten geeignete Sicherheitskontrollen und Authentifizierungsmechanismen zu installieren.

**Was Einzelhändler noch tun sollten**
Außerdem sollten Händler Informationssicherheitspläne für ihre Beschäftigten ins Leben rufen und deren Berücksichtigung durch Vorgesetzte und Teamleiter prüfen lassen.

Obwohl das Problem mit unsicheren Passwörtern mittlerweile sowohl Privatleuten als auch Unternehmern bekannt sein dürfte, ist es immer noch keine Seltenheit, dass leicht zu erratende Kennwörter wie "12345", "Passwort" oder das eigene Geburtsdatum verwendet werden.

**Passwörter werden mehrmals genutzt**
Dazu kommt, dass die Nutzer sie ebenfalls bei anderen Online-Konten nutzen. Das spielt Angreifern, die das Kennwort einmal geknackt haben, natürlich ideal in die Hände. Ebenso riskant ist es, die Kombinationen nicht regelmäßig zu verändern oder sie an unsicheren Orten aufzubewahren.

Nützliche Passwort Manager-Tools helfen dabei, komplexe Zahlen-Buchstaben-Kombinationen zu generieren, abzurufen und in einer verschlüsselten Datenbank zu speichern.

**Die Datenschutzverordnung im Einzelhandel**
Des Weiteren erinnern sie an eine regelmäßige Aktualisierung des Kennwortes. Es ist ratsam, mit allen Mitarbeitern eine Passwort-Schulung durchzuführen und ihnen mit Hinweisfenstern den Anmeldevorgang zu erleichtern.

**Unzureichender Schutz bei Administrationskonten**
Besonders fatal sind unsichere Zugangsdaten bei Accounts, die über eine hohe Anzahl an Zugriffsrechten verfügen. Die Inhaber solcher Konten tragen häufig eine große Verantwortung für den reibungslosen Ablauf geschäftlicher Prozesse sowie für die Verwaltung sensibler Daten. Greifen Hacker auf diese Accounts zu, umgehen sie potenzielle IT-Systeme und fangen die begehrten Informationen direkt ab.

Um das zu verhindern, macht es Sinn, alle Konten zunächst mit denselben Privilegien auszustatten. Je nach Position und Aufgaben des jeweiligen Angestellten im Unternehmen können die Befugnisse schließlich Stück für Stück erweitert werden.

Für freiberufliche Mitarbeiter, die an gemeinsamen Projekten beteiligt sind, empfiehlt sich ein zeitlich begrenztes Zugriffsrecht. Accounts von Administratoren sollten generell nur zur Organisation einzelner Firmenbereiche zum Einsatz kommen. Zusätzlich sind auch hier Mehrfach-Authentifizierungen beim Einloggen durchzuführen.

**Schutz der Kundendaten**
Die digitale Kommunikation mit Kunden, Lieferanten, Geschäftspartnern und Mitarbeitern hat im Handel innerhalb der letzten Jahre stark zugenommen. Ebenso wie die Nutzung von Online-Servern und Cloud-Programmen, die ein flexibles Arbeiten überall möglich machen.

Zusammen mit diesen Entwicklungen hat sich jedoch genauso das Risiko für Cyberangriffe und Datenklau erhöht, da im Netz die größten Bedrohungen lauern. Denn viele Firmen sind hinsichtlich ihrer Datensicherheit intern gut aufgestellt, wohingegen Schutzmaßnahmen gegen Zugriffe von Dritten nur spärlich vorhanden sind.

Dabei sind gerade die Kundeninformationen im Online-Handel besonders schützenswert und unterliegen eindeutig festgelegten gesetzlichen Rahmenbedingungen.

**Datenschutz: Mitarbeiter mit einbeziehen**
Mit zertifizierten Softwarelösungen zur Unternehmenssteuerung sowie nützlichen Passwort Manager-Systemen gehen Händler den ersten Schritt in Richtung sichere Datenverwaltung. Doch selbst die beste Softwareanwendung und zahlreiche Verschlüsselungen können menschliche Fehler nicht unterbinden.

Deshalb ist es unerlässlich, die Mitarbeiter in das Thema Datenschutz miteinzubeziehen. Unternehmer sollten regelmäßige Schulungen und Fortbildungen abhalten, damit ihr Personal in der Lage ist, Angriffsversuche als solche zu erkennen und zu umgehen.

Auch Kontrollmechanismen und Simulationstests sollten dabei nicht fehlen. Einen 100-prozentigen Schutz wird es niemals geben, doch mit den genannten Maßnahmen sind Betriebe im Handel bestens gerüstet, um schwerwiegende Konsequenzen wie Imageverluste und Klagen weitestgehend zu vermeiden.