FAKTENBLATT

Shred-it's Leitfaden zur Wiederherstellung der Datensicherheit nach den Sommerferien

In den Sommermonaten nehmen die Mitarbeiter ihren wohlverdienten Jahresurlaub. Wenn sie jedoch zurückkehren, sollten Unternehmen ihre Mitarbeiter daran erinnern, wie sie mit vertraulichen Informationen umgehen müssen, um das Risiko einer Datenverletzung zu verringern.

WUSSTEN SIE SCHON...

dass die durchschnittlichen Kosten einer Datenschutzverletzung 3,533,430 Euro betragen? [1] Und dass 31 % der Verbraucher das Vertrauen in ein Unternehmen verlieren würden, das von einer Datenschutzverletzung betroffen ist? [2]

Im Folgenden finden Sie einige der besten Möglichkeiten, wie Mitarbeiter nach dem Sommerurlaub bewährte Verfahren zur Datensicherheit nutzen können.

1. **Minimieren Sie die Menge der auf einem mobilen Gerät gespeicherten Informationen** nur auf das, was für die Arbeit benötigt wird.
2. **Seien Sie aufmerksam, wenn Sie aus der Ferne arbeiten** in einem Café, einer Flughafenlounge oder einem Bus. Legen Sie Ihre Arbeit beiseite oder wechseln Sie den Platz, wenn sich jemand verdächtig verhält.
3. **Vermeiden Sie die gemeinsame Nutzung elektronischer Geräte mit Familie, Freunden und anderen Besuchern.** Schließen Sie sie weg, wenn sie nicht benutzt werden. Bewahren Sie sensible und vertrauliche Unterlagen ebenfalls an einem sicheren Ort auf.
4. **Achten Sie auf Phishing-E-Mails und bösartige Websites.** Zu den Anzeichen gehören Rechtschreib- und Grammatikfehler, verdächtige E-Mail-Adressen und dringende Aufforderungen zum Handeln. Senden Sie niemals persönliche Daten wie Namen, Adresse und Kreditkartendaten per E-Mail.
5. **Befolgen Sie die Unternehmensverfahren für die sichere Entsorgung von digitalen und gedruckten Informationen.** Werfen Sie kein Papier in Mülltonnen oder Recycling-Container. Werfen Sie ausgediente elektronische Geräte nicht einfach in den Müll oder recyceln Sie sie. Bringen Sie sie nach der Sommerpause zur sicheren Entsorgung ins Büro.
6. **Verwenden Sie keine unbekannten USB-Geräte.** Verwenden Sie nur vom Unternehmen zugelassene Geräte.
7. **Lassen Sie mobile Geräte niemals unbeaufsichtigt** in der Öffentlichkeit oder sichtbar in einem verschlossenen Fahrzeug.
8. **Software aktualisieren und Patches sofort installieren.** Untersuchungen haben ergeben, dass 82 % der entdeckten Sicherheitsverletzungen auf die Nichtaktualisierung von Software-Patches zurückzuführen sind. [3]
9. **9 Verstärken Sie Passwörter auf allen Geräten und Konten** (lange Zeichenfolge, die Ziffern, Buchstaben und Symbole enthält). Über 60 % der Sicherheitsverletzungen sind auf missbräuchlich genutzte Zugangsdaten zurückzuführen. [4]
10. **Schalten Sie die Wi-Fi- und Bluetooth-Konnektivität aus, wenn sie nicht verwendet wird.** Um vertrauliche Daten zu übertragen oder eine Verbindung zum Büro herzustellen, verwenden Sie persönliche Hotspots, ein virtuelles privates Netzwerk (VPN) oder passwortgeschützte Wi-Fi-Netzwerke. Bei einer Verbindung über Bluetooth werden die Daten verschlüsselt.

1 IBM: Bericht über die Kosten einer Datenpanne 2021
2 Shred-it: Datenschutzbericht 2022
3 Voke Media: Secure Operations Automation Market Snapshot Report 2017
4 Verizon: Data Breach Inverstions Report 2022

Wenn Sie mehr über bewährte Verfahren zur Gewährleistung der Sicherheit erfahren möchten, besuchen Sie Shredit.de oder rufen Sie 0808 239 4478 an.

Wir schützen das, was wirklich zählt.

Shred-it®
Ein Unternehmen von Stericycle®