Datenleck von unterwegs: Vier Security-Massnahmen für mobiles Arbeiten

Für viele Mitarbeiter ist das Arbeiten von unterwegs oder aus dem Home-Office zur Selbstverständlichkeit geworden. Die Sicherheitsrisiken werden dabei jedoch oft übersehen: Auf Laptops, Mobiltelefonen und Tablets befinden sich häufig sensible Unternehmensdaten wie vertrauliche E-Mails und Dokumente, personenbezogene Daten oder Finanzinformationen. Durch ein gestohlenes oder verlorenes Gerät steigt das Risiko eines Datenlecks. Nach der DSGVO stellt der Verlust eines mobilen Firmengeräts mit personenbezogenen Daten eine Datenschutzverletzung dar, die mit Bussgeldern von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Gesamtjahresumsatzes geahndet werden kann.
Es ist unmöglich, den Verlust mobiler Endgeräte durch Mitarbeiter komplett zu verhindern. Um das Risiko eines Datenlecks zu minimieren, mag es verlockend erscheinen, mobiles Arbeiten einzuschränken. Doch dies kann sich negativ auf die Produktivität und Mitarbeiterzufriedenheit auswirken. Flexibles Arbeiten ist heutzutage für viele Mitarbeiter eine Selbstverständlichkeit, daher ist es wichtig, dass Unternehmen entsprechende Richtlinien und Sicherheitsmassnahmen einführen.

1. Entwicklung von Richtlinien für mobiles Arbeiten

? Anwendungen und Informationen, auf die Mitarbeiter per Mobilgerät zugreifen dürfen
? Mindestanforderungen der Sicherheitskontrollen für Mobilgeräte
? Vom Unternehmen bereitgestellte Komponenten wie SSL-Zertifikate zur Geräteauthentifizierung
? Unternehmensrechte für Ä„nderungen auf Mobilgeräten wie ein Remote-Wipe verlorener oder gestohlener Devices. Dazu gehören die Haftung des Unternehmens für die personenbezogenen Daten eines Mitarbeiters, falls ein Gerät aus Sicherheitsgründen gelöscht werden muss, sowie die Haftung des Mitarbeiters für den Verlust sensibler Unternehmensdaten, die durch Fahrlässigkeit oder Missbrauch des Mitarbeiters verursacht wurden.
? Regelmässige Sicherung und sachgemässe Speicherung von Unternehmensdaten

2. Verschlüsselung von Geräten, E-Mails und sensiblen Daten

Da Daten durch BYOD (Bring Your Own Device) aus dem Kontrollbereich vieler Security-Massnahmen geraten, ist es wichtig, dass Unternehmen sensible Daten sowohl im Ruhezustand als auch bei Äœbertragung verschlüsseln. Entsprechende Data Security-Lösungen ermöglichen die Verschlüsselung von Geräten, E-Mails sowie Daten, und häufig wird die Encryption-Funktion mit Kontroll- und Äœberwachungsfunktionen verbunden. Data Security-Software versieht proaktiv sensible Informationen in E-Mails sowie Anhänge mit einem Security-Tag, klassifiziert und verschlüsselt sie. Dies bietet eine adäquate Antwort auf die Sicherheitsherausforderungen durch gesetzliche Regelungen, Remote-Arbeitskräfte, BYOD und Projekt-Outsourcing.

3. Äœberwachung und Kontrolle durch Data Loss Prevention (DLP)

Remote und mobiles Arbeiten hat den traditionellen Netzwerkperimeter nahezu überflüssig gemacht. Unternehmen müssen sich nicht mehr nur auf die Sicherung des Perimeters, sondern auch auf die Sicherung von Daten konzentrieren, unabhängig davon, wo diese sich gerade befinden. Data Loss Prevention (DLP) umfasst eine Reihe von Tools und Prozessen, die sicherstellen, dass sensible Daten nicht verloren gehen, missbraucht oder von unbefugten Benutzern abgerufen werden. DLP-Software klassifiziert vertrauliche und geschäftskritische Daten und identifiziert Verstösse gegen die von Unternehmen definierten Richtlinien oder gesetzlichen Regelungen wie der DSGVO.

Sobald Sicherheitsverstösse identifiziert werden, erzwingen DLP-Tools deren Behebung durch Warnmeldungen, Verschlüsselung und weiteren Schutzmassnahmen, um zu verhindern, dass Mitarbeiter aus Versehen oder mit böswilliger Absicht sensible Daten weitergeben. DLP überwacht und kontrolliert auch Endpunkt-Aktivitäten, filtert Datenströme in Unternehmensnetzwerken und überwacht Daten in der Cloud, um diese im Ruhezustand sowie bei Äœbertragung und Gebrauch zu schützen. Dies verschafft Sicherheitsteams einen umfangreichen Einblick, wenn Mitarbeiter versuchen, Daten in einer Weise zu bewegen, die gegen Sicherheits- oder Datenschutzrichtlinien verstösst, und blockiert den Vorgang.

4. Mitarbeiter schulen

Regelmässige Schulungen können Mitarbeitern helfen, die Risiken und potenziellen Folgen des Verlusts eines mobilen Endgeräts zu verstehen und vorsichtig zu agieren. Im Rahmen dieser Schulungen ist es auch wichtig, die Bedeutung einer rechtzeitigen Meldung von verloren gegangenen oder gestohlenen Geräten hervorzuheben.
Mobiles Arbeiten ist ein wichtiger Bestandteil heutiger Unternehmenskultur. Auch wenn nicht verhindert werden kann,

dass Mitarbeiter Geräte verlieren, kann die Wahrscheinlichkeit eines Datenlecks minimiert werden. Durch die oben genannten Best Practices wie Mitarbeiterschulungen, festgelegte Richtlinien und den Fokus auf datenzentrierte Sicherheitstechnologien können Unternehmen das Sicherheitsrisiko durch verlorene und gestohlene Geräte erheblich einschränken.