MOBILES ARBEITEN:

Vier Security-Maßnahmen ...

Besonders im Bauhandwerk arbeiten viele Mitarbeiter von unterwegs, auf der Baustelle oder im Baubüro. 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 Gesamtjahresumsatzes geahndet werden kann ... *von Christoph M. Kumpa*

Es ist unmöglich, den Verlust mobiler Endgeräte durch Mitarbeiter komplett zu verhindern. Um das Risiko eines Datenlecks zu minimieren, ist es wichtig, im Betrieb entsprechende Richtlinien und Sicherheitsmaßnahmen einzuführen.

1. Entwicklung von Richtlinien für mobiles Arbeiten: Mitarbeiter müssen klar über die Regeln und Best Practices ihres Unternehmens in Bezug auf mobiles Arbeiten informiert werden. Die Richtlinien sollten folgende Punkte abdecken:

Christoph M. Kumpa, Director DACH & EE bei Digital Guardian

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 Änderungen 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

Bild: Digital Guardian

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 Übertragung verschlüsseln. Entsprechende Data Security-Lösungen ermöglichen die Verschlüsselung von Geräten, E-Mails sowie Daten, und häufig wird die Encryption-Funktion mit Kontroll- und Überwachungsfunktionen 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. Überwachung 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 verlorengehen, 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 weitere 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 Übertragung 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 potentiellen 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 verlorengegangenen oder gestohlenen Geräten hervorzuheben.

FAZIT

Mobiles Arbeiten ist ein wichtiger Bestandteil im Bauhandwerksbetrieb. Auch wenn nicht verhindert werden kann, daß Mitarbeiter Geräte verlieren, kann die Wahrscheinlichkeit eines Datenlecks minimiert werden: z. B. mit Mitarbeiterschulungen, festgelegten Richtlinien sowie datenzentrierten Sicherheitstechnologien. <<