

HANDSCHUHE, GETEILTE TABLETS, FUNKLOCH:

Wie Handwerksbetriebe ihre Geräte auf der Baustelle absichern

Monteure entsperren Tablets mit nassen Handschuhen, vier Mann teilen sich ein Baustellen-Tablet, Kundenfotos liegen ohne Empfang nur lokal auf dem Gerät. Der Beitrag zeigt, welche Einstellungen im Betrieb halten, was die Geräteverwaltung einen Achtpersonenbetrieb kostet und wie Zugänge beim Austritt enden ... | VON THOMAS JOOS

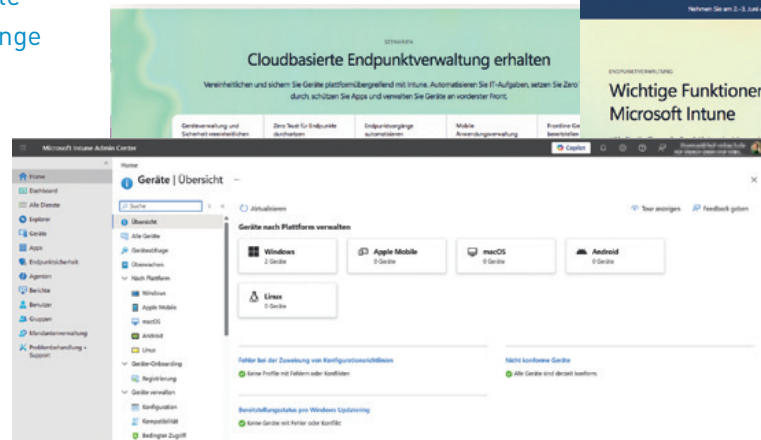
Für die HDI Cyberstudie 2026 hat Sirius Campus rund 1.100 Entscheider aus dem Mittelstand befragt. 64 % der angegriffenen Betriebe nennen Phishing-Mails als häufigste Methode, die durchschnittliche Schadenshöhe bei erfolgreichen Angriffen liegt bei rund 25.000 Euro, bei Betrieben mit Präventionsmaßnahmen fällt sie im Schnitt 33 Prozent niedriger aus (<https://www.cash-online.de/a/hdi-kmu-cyberstudie-2026-weniger-schaeden-aber-neue-risiken-721775/>). Auf der Baustelle scheitert Prävention selten an fehlendem Wissen. Sie scheitert an Nässe und an Geräten ohne festen Besitzer und Verantwortlichkeiten.

Der Sperrbildschirm unter Baustellenbedingungen

Fingerabdrucksensoren erkennen nasse oder staubige Finger nicht. Gesichtserkennung scheitert am Helm mit Schutzbrille. Der übliche Reflex ist die Abschaltung der Bildschirmsperre, und danach genügt einem Finder ein Wischen über das Display, um Kundenadressen und Firmenpostfach zu öffnen. Betriebe sollten die Sperre erhalten und die Zeit bis zur automatischen Sperrung von 30 Sekunden auf zwei bis fünf Minuten heraufsetzen, als Zugang bleibt eine sechsstellige PIN, die auch mit Handschuh funktioniert. Robuste Android-Geräte bieten zusätzlich eine erhöhte Touch-Empfindlichkeit für Arbeitshandschuhe. Über Microsoft Intune lässt sich beides zentral vorgeben, die Mindestlänge der PIN als Konformitätsregel und die Zeit bis zur Sperrung als Konfigurationsprofil (<https://learn.microsoft.com/de-de/microsoft-365/admin/security-and-compliance/m365bp-devices-enrollment?view=o365-worldwide>).

Ein Tablet für mehrere Monteure

Auf vielen Baustellen liegt ein Tablet, das der Polier morgens ausgibt und abends einsammelt, im Bauwagen. Ein gemeinsames Konto mit gemeinsamem Passwort löst die Anmeldung und schafft ein neues Problem, denn nach einem Vorfall lässt sich nicht mehr zuordnen, wer welche Datei geöffnet oder gelöscht hat. Android Enterprise kennt für solche Geräte den Registrierungstyp „dediziertes Gerät“. In Verbindung mit dem Modus für gemeinsam genutzte Geräte meldet sich jeder Monteur mit dem eigenen Konto an, beim Abmelden räumt das System die Daten der Sitzung aus den beteiligten Apps (<https://learn.microsoft.com/de-de/intune/solutions/frontline-worker/android>).



Geräteverwaltung ohne eigene IT-Abteilung

Ein Betrieb mit acht Beschäftigten hat keine IT-Abteilung, oft nicht einmal einen festen Dienstleister. Microsoft 365 Business Premium enthält Intune Plan 1, die Geräteverwaltung steckt damit in einer Lizenz, die viele Betriebe ohnehin zahlen (<https://www.microsoft.com/de-de/microsoft-365/business/microsoft-365-plans-and-pricing>). Die Lizenzfrage ist im Handwerk selten das Hindernis, häufiger bleibt eine einmal eingerichtete Richtlinie nach dem ersten Gerätewechsel unangetastet stehen. Ungeklärt bleibt zudem, wer das gestohlene Smartphone um 22 Uhr sperrt, deshalb sollten Betriebe eine Reaktionszeit für Gerätesperrung und Fernlöschung schriftlich vereinbaren und eine zweite Person im Betrieb mit Zugang zum Verwaltungsportal ausstatten.

Funkloch, lokale Daten und Sicherung

Im Keller eines Rohbaus gibt es keine Verbindung. Fotos vom Aufmaß und markierte Pläne liegen dann lokal auf dem Gerät. Android und iOS verschlüsseln den Speicher ab Werk, sobald eine Bildschirmsperre gesetzt ist. Bei Windows-Tablets sollte der Betrieb BitLocker aktivieren und den Wiederherstellungsschlüssel in Entra ID hinterlegen, denn ein nur lokal abgelegter Schlüssel nützt nach einem Gerätedefekt niemandem mehr. Sobald das Gerät wieder Netz hat, holt die Synchronisierung mit OneDrive oder SharePoint die Dateien nach, eine Datensicherung ersetzt sie damit nicht, denn eine gelöschte oder verschlüsselte Datei repliziert die Synchronisierung ungeprüft in die Cloud.

Geräterückgabe und Zugriff von Nachunternehmern

Beim Austritt eines Monteurs stehen in Intune zwei Aktionen zur Auswahl. „Wipe“ setzt das Gerät auf den Werkzustand zurück und paßt



zu Firmengeräten. „Retire“ löscht ausschließlich Firmendaten und Arbeitsprofil und paßt zu privaten Geräten mit Arbeitsprofil. Nachunternehmer sollten kein Firmenkonto bekommen, für Pläne und Fotos genügen Freigabelinks mit Ablaufdatum, deren Berechtigung nach der Abnahme wieder entfernt wird. Die Verantwortung nach DSGVO bleibt in jedem Fall beim Betrieb, unabhängig davon, wem das Gerät gehört.

FAZIT

Die Technik steckt bei den meisten Betrieben bereits in vorhandenen Lizenzen. Der Aufwand liegt in der Einrichtung und in der Erreichbarkeit im Notfall. Sind personenbezogene Daten betroffen, verlangt Artikel 33 DSGVO eine Meldung an die zuständige Datenschutzbehörde des Bundeslandes binnen 72 Stunden (<https://www.nextlevel-handwerk.de/2026/07/20/handlungsplan-bei-einem-cyberangriff/>). Kostenfreie Checks und eine Notfallhilfe bietet die staatlich geförderte Transferstelle Cybersicherheit im Mittelstand (<https://transferstelle-cybersicherheit.de/>). <<