7 praktische Tips für mehr **IT-Sicherheit** im Handwerk

Ob Elektriker, Tischler oder Installateur: Viele Handwerksprofis arbeiten von unterwegs, auf der Baustelle oder beim Kunden vor Ort. Laptops, Tablets und Smartphones entwickeln sich zum unverzichtbaren Begleiter, doch die Sicherheitsrisiken werden oft übersehen: Auf mobilen Endgeräten befinden sich sensible Unternehmensinformationen, etwa Kunden- und Auftragsdaten oder Baupläne und Patente – es besteht das Risiko, daß sie zu Einfallstoren für Malware oder Viren werden, die sich anschließend im Unternehmensnetzwerk verbreiten ... | VON TUNCAY SANDIKCI

Warum Handwerksbetriebe jetzt handeln sollten

Die Gefahr wächst. Cyberattacken nehmen weltweit zu und verursachen immer höhere wirtschaftliche Schäden: Der Digitalverband Bitkom geht davon aus, daß Cyberangriffe die deutsche Wirtschaft jährlich über 220 Milliarden Euro kosten. In Deutschland lag der Anteil der Unternehmen, die in den vergangenen zwölf Monaten eine solche Attacke erlebt haben, laut Lagebericht für 2022 des BSI (Bundesamt für Sicherheit in der Informationstechnik) bei 46 Prozent. Gerade kleine und mittlere Unternehmen (KMU) bieten große Angriffsflächen für Cyberkriminelle. Sie sind, so das BSI, gegenüber größeren Firmen hinsichtlich ihrer IT-Sicherheit schlechter aufgestellt. Doch Cyberattacken können existenzbedrohende Auswirkungen für die Handwerksbranche haben. Phishing-Mails etwa zielen darauf ab, Zugangsdaten zu stehlen oder Malware zu installieren. Diese bösartige Software nutzt Sicherheitslücken von Computern, Tablets und Smartphones aus, um Schäden zu verursachen. Das gilt besonders für Angriffe über mobile Geräte, weil viele Endpunkte innerhalb betrieblicher IT-Infrastrukturen nicht ausreichend stark geschützt sind. Passwörter können gehackt, sensible Daten gestohlen werden. Ganze Systeme werden von jetzt auf gleich arbeitsunfähig.

So können sich Betriebe schützen

Doch wie gelingt es, mobile Infrastrukturen effizient zu schützen – ohne, daß spezielle Security-Expertise im Betrieb vorgehalten werden muß? Die gute Nachricht: Mit diesen praktischen Maßnahmen läßt sich die IT-Sicherheit von Tablet, Smartphone & Co. erhöhen.

1. Regelmäßige Updates fahren: Damit Mitarbeiter in sicheren Systemen arbeiten können, sollten Betriebssystem und Anwendungen automatisch in regelmäßigen Abständen aktualisiert werden. Mit den Sicherheitsupdates beheben Hersteller meist neben Bugs auch Schwachstellen, die zu einem erhöhten Sicherheitsrisiko führen können.

2. Datensicherung ist Pflicht: Regelmäßige Backups sowie die Sicherung von Daten an verschiedenen Orten schützen nicht nur vor Datenverlust, sondern auch vor Ransomware, die von Cyberkriminellen zu Erpressungszwecken verwendet wird.

3. Sensible Daten verschlüsseln: Personenbezogene Informationen und Geschäftsgeheimnisse sollten standardmäßig mit einer starken Verschlüsselung vor fremden Zugriffen geschützt sein. Das mobile Betriebssystem Android bietet seit Version 7.0 mit der dateibasierten Verschlüsselung (FBE, File-based Encryption) bereits einen Basisschutz. Samsung ergänzt die Sicherung von Gerätedaten mit der Knox Suite durch zusätzliche kryptographische Schlüssel.

Tuncay Sandikci ist Director MX B2B bei Samsung Electronics GmbH

4. Übertragungswege schützen: Daten können nicht nur direkt auf den Geräten selbst, sondern auch bei der Übermittlung gestohlen werden, Schadsoftware schleust sich ein. Besonders gefährlich sind offene WLAN-Umgebungen. Daher gilt: Vertrauliche Daten möglichst nur über ein VPN (Virtual Private Network) abrufen. Für den professionellen Einsatz empfehlen sich Lösungen wie das Samsung Knox VPN Framework, das angepaßte Funktionen und eine starke Verschlüsselung bietet.

5. Einfaches UEM mit Partnern lösen: Hinter Unified Endpoint Management verbirgt sich die einheitliche Verwaltung und Überwachung von Endnutzergeräten innerhalb >>

Bilder: Samsung

IMPRESSUM

Computern im Handwerk/ handwerke.de
gegründet 1984, dient als unabhängiges Fachmagazin für moderne Kommunikation den Betrieben der **Bauhaupt- und Nebengewerbe** im „portionierten" Wissens- und Technologie-Transfer.

Herausgeber: Horst Neureuther

© Copyright: CV München
CV Computern-Verlags GmbH
Goethestraße 41, 80336 München

Telefon o 89/54 46 56-0
Telefax o 89/54 46 56-50
Postfach 15 06 05, 80044 München
E-Mail: info@cv-verlag.de
redaktion@cv-verlag.de
www.handwerke.de

Geschäftsleitung:
Dipl.-Vw. H. Tschinkel-Neureuther

Anzeigenleitung:
Dipl.-Vw. Heide Tschinkel-Neureuther
e-mail: anzeigen@cv-verlag.de

Redaktion und redaktionelle Mitarbeiter in dieser Ausgabe:
Frédéric Baroin, Nora Bax, Birgit Blumberg-Bohn, Ann-Kathrin Gräfe, Thomas Hey, Stella Lapichino, Margrit Lingner, Verena Mikeleit, Jasmin Möser, Nadja Müller, Horst Neureuther (verantw.), Myrko Rudolph, Gundo Sanders, Tuncay Sandikci, Romy Schächtel, Sonia Welter

Anzeigenvertretung:
Medienmarketing SANDERS

Layout:
AD&D Werbeagentur GmbH, Silvia Romann, Dietmar Kraus

Druck:
Walstead NP Druck GmbH, St. Pölten

Druckauflage: 50.500
Tatsächliche Verbreitung: 50.272 (II/23)

Auflage und Verbreitung kontrolliert.

39. Jahrgang
Erscheinungsweise: 10 x jährlich

Abo-Preis:
29,– € p.a. plus Porto inkl. MwSt.

Einzelpreis: 2,90 €
Ein Abonnement verlängert sich automatisch um ein Jahr, wenn es nicht spätestens 3 Monate vor Ablauf des Bezugszeitraumes gekündigt wird.

ISSN 0931-4679
Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) Berlin

Zur Zeit gilt die Anzeigenpreisliste Nr. 40 vom 01.11.2022.

Titelkopf: © Fotolia.de/yellowj

>> eines Unternehmens. UEM gilt als erste Verteidigungslinie gegen bösartige Apps. Ein ordnungsgemäß verwaltetes Gerät kann die Möglichkeit für die Installation von potentiell schädlichen Apps und Attacken erheblich reduzieren. Bei der Umsetzung helfen Services wie die Samsung Knox Suite oder externe IT-Partner.

6. Auf passende Hardware setzen: Gute IT-Sicherheit ist mehr als reine Cyberabwehr. Ebenso sinnvoll ist es, Hardware anzuschaffen, die auch herausfordernden Bedingungen standhält und die Mitarbeiter überall hinbegleiten kann. Die robusten Geräte der Samsung Ruggedized-Serie sind wasser-, staub- und stoßresistent und erfüllen den Militärstandard MIL-STD-810G[1]. Kunden profitieren dabei von zwei Jahren Produktlebenszyklus und fünf Jahren Softwareupdate-Support ab globaler Markteinführung.

7. Belegschaft sensibilisieren: Menschliches Versagen kann auch die Ursache für einen Cyberangriff sein. Unachtsamkeit oder Unwissen öffnen Hackern Tür und Tor. Dafür reicht oft nur ein Klick auf einen bösartigen Link in einer E-Mail. Wichtig ist, das Team für diese Gefahren zu sensibilisieren und regelmäßig zu schulen.

Mobile Sicherheit braucht eine starke Plattform

Samsung denkt das Thema Sicherheit bei seinen Smartphones und Tablets von Anfang an mit – und stellt mit der Knox Plattform auf jeder Ebene sicher, daß vertrauliche und sensible Daten geschützt bleiben. Die robuste Plattform hilft, die mobile IT-Infrastruktur von Unternehmen abzusichern und schützt vor Datenlecks, Cyberangriffen und Viren.
Ein zentrales Asset ist hier Knox Vault: Die Funktion bietet eine nach EAL5+ zertifizierte, manipulationsgeschützte Umgebung, in der die wichtigsten Daten auf dem Gerät geschützt aufbewahrt werden. Sie isoliert PINs, Passwörter, biometrische Daten und sicherheitskritische Schlüssel fernab von den restlichen Daten in einem gesicherten Speicher.

Klar ist: Auch im Handwerk werden immer mehr Prozesse digitalisiert. Das bedeutet neue Chancen, gleichzeitig steigen auch die Sicherheitsgefahren, denn Cyberattacken werden immer raffinierter. Plattformen wie Samsung Knox bieten gute Voraussetzungen dafür, daß Unternehmen – unabhängig davon, ob groß oder klein – die Risiken der Smartphone- und Tablet-Nutzung in den Griff bekommen, wenn sie diese zentral managen und schützen. <<

[1] MIL-STD-810G ist eine Militärnorm, die standardisierte Prüfmethoden festlegt, um die Widerstandsfähigkeit von Endgeräten zu testen (z. B. gegen Stürze, Vibration, Eindringen von Mikropartikeln). Getestet wurde das Gerät auf folgende Einflüsse: Hoch- und Niedrigtemperatur, Vibration, Luftdruck, Salznebel, Luftfeuchtigkeit, Staub, mechanischer Schock, Einfrieren, solare Einstrahlung. Weitere Informationen unter www.atec.army.mil/publications/Mil-Std-810G/MIL-STD-810G.pdf