MOBILE GERÄTE IN DER FIRMA: LEITFADEN FÜR KLEINE UND MITTLERE UNTERNEHMEN

Mobile Geräte sind aus dem Unternehmensalltag nicht mehr wegzudenken, dabei bringt der Einsatz auch einige Risiken mit sich. Mit wenig Aufwand lassen sich allerdings wirksame Strategien entwickeln, um auf Vorfälle wie z.B. den Verlust eines Gerätes vorbereitet zu sein. **Die wichtigsten Punkte fassen wir Ihnen hier zusammen!**

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

DIGITAL SICHER NRW

WIE MOBILE GERÄTE ZU EINER GEFAHR WERDEN KÖNNEN

GRUND 1: ÖFFENTLICHES W-LAN

Die Nutzung von öffentlichen Netzwerken kann zum Sicherheitsrisiko werden, denn von außen lässt sich nicht erkennen, wie diese genau funktionieren. So können Verkehrsdaten vom Betreiber oder von Angreifern mitgeschnitten und eingesehen werden.

GRUND 2: ÖFFENTLICHE LADESTATIONEN

Auch das Verwenden von öffentlichen Ladestationen stellt ein mögliches Sicherheitsrisiko für Unternehmen dar, denn über das Ladekabel kann Schadsoftware auf das angeschlossene Gerät gelangen oder z.B. durch eine Überspannung beschädigt werden.

DIGITAL SICHER NRW

WIE MOBILE GERÄTE ZU EINER GEFAHR WERDEN KÖNNEN

GRUND 3: PHISHING-MAILS

Mit Hilfe von Phishing-Mails können Kriminelle Login-Namen und Passwörter von Accounts oder andere sensible Informationen abgreifen. Dies erfolgt in der Regel durch die Installation von Schadsoftware, durch die sich Hacker Zugriff zum Gerät verschaffen.

GRUND 4: APPS

Mit der Installation von Apps können sich Betreiber weitreichende Berechtigungen einholen. Durch Werbung und dem sogenannten „Tracking“ kommt es dabei zu einer Verletzung der Privatsphäre. Apps können zudem Schadsoftware enthalten, mit der z.B. Passwörter oder Zugangscodes zu Bankkonten abgegriffen werden können. Hacker können dafür auch Sicherheitslücken innerhalb der Apps nutzen.

DIGITAL SICHER NRW

WIE MOBILE GERÄTE ZU EINER GEFAHR WERDEN KÖNNEN

GRUND 5: VERLORENES GERÄT

Ohne eine Absicherung (z.B. Passwort, Fingerabdruck oder Face-ID) können Dritte im Fall eines Geräteverlusts auf alle Unternehmensdaten – inklusive vertraulicher Mails, Bilder, Dateien, Kontaktdaten – zugreifen. Angreifern stehen dadurch alle Möglichkeiten offen, das Unternehmen zu gefährden.

GRUND 6: FEHLENDE VERSCHLÜSSELUNG

Ein Passwort schützt i.d.R. nur das Gerät, nicht die darauf gespeicherten Daten. Für Daten auf dem Smartphone-Speicher gilt, dass das Gerät lediglich via USB mit dem PC verbunden werden muss, um darauf befindliche Daten auszulesen. Gesicherte Daten auf einer separaten Speicherkarte können durch das Entfernen dieser ebenfalls ausgelesen werden.

WIE SIE IHRE MOBILEN GERÄTE SCHÜTZEN

DIGITAL SICHER NRW

1. SICHERE GRUNDKONFIGURATION

- Deaktivieren Sie die feste Werbe-ID.
- Aktivieren Sie den Standort nur, wenn notwendig und schalten Sie Ihren Standortverlauf / Wichtige Orte aus.
- Deaktivieren Sie Roaming, um sich vor kostenpflichtigem SMS-Versand im Ausland zu schützen.
- Schränken Sie die Datenweitergabe / Telemetrie ein.

2. VERWENDEN EINES ZUGRIFFSCHUTZES

- Nutzen Sie möglichst mehr als 4 Zeichen bei der PIN bzw. mehr als 4 Punkte beim Muster.
- Setzen Sie Passwörter nach den üblichen Regeln. Je länger desto besser!
- Ein Fingerabdruck bzw. eine Gesichtserkennung ermöglicht Ihnen ein komfortables entsperren und damit ein komplexes Passwort, PIN oder Muster.

3. EINSCHRÄNKEN VON APP-BERECHTIGUNGEN

- Hinterfragen Sie, welche App welche Berechtigungen wirklich benötigt!
- Nehmen Sie nicht notwendige Berechtigungen wieder zurück.

WIE SIE IHRE MOBILEN GERÄTE SCHÜTZEN

DIGITAL SICHER NRW

4. UPDATES DURCHFÜHREN

- Aktivieren Sie die automatische Installation von Updates.
- Installieren Sie neue Updates immer zeitnah nach der Benachrichtigung.
- Stoßen Sie die Suche nach Updates zur Sicherheit regelmäßig selbstständig an.

5. NICHT-PERSONALISIERTE GERÄTENAMEN

- Achten Sie darauf, dass Firmengeräte keine Hinweise auf die Institution oder den Benutzenden enthalten.

6. SPRACHASSISTETEN DEAKTIVIEREN

Verhindern Sie, dass Befehle von Dritten - wie beispielsweise ein ungewollter Einkauf - ausgeführt werden können, indem Sie die Sprachassistenten an Ihren Geräten ausschalten. Ein weiterer Grund für eine Deaktivierung ist, dass Sprachassistenten im Hintergrund häufig versehentlich Gesprächsdaten aufzeichnen.

WIE SIE IHRE MOBILEN GERÄTE SCHÜTZEN

DIGITAL SICHER NRW

Für den Umgang mit mobilen Geräten sollten Sie in Ihrem Unternehmen **verbindliche Regelungen** schaffen und **Verantwortlichkeiten festlegen**. Dabei sollte immer auch der **Umgang mit gestohlenen bzw. verlorenen Geräten** bedacht werden.

7. VERWENDUNG VON WERBEBLOCKERN

- Auch angezeigte Werbung kann schadhaften Code enthalten. Davor können aktuell gehaltene Werbeblocker schützen.
- Greifen Sie auch zum Schutz vor „Tracking“ auf Werbeblocker im Browser zurück.

8. SENSIBILISIERUNG FÜR GEFÄHRDUNGEN

- Ermöglichen Sie Ihren Mitarbeitenden die regelmäßige Teilnahme an Schulungen zu Sicherheitsaspekten.

WIE SICH MOBILE GERÄTE SICHER VERWALTEN LASSEN: DAS MOBILE DEVICE MANAGEMENT

EIN MOBILE DEVICE MANAGEMENT (MDM) ERMÖGLICHT…

- die Verschlüsselung sensibler Daten,
- die Durchführung automatisierter Sicherungen,
- die Inventarisierung von Hard- und Software,
- die Verteilung und Anwendung von „Sicherheitspolicies“ (Vorgaben),
- eine Trennung zwischen privater und geschäftlicher Nutzung,
- eine Ortung, Sperrung oder Fernlöschung der mobilen Geräte.

Mit Hilfe eines **Mobile Device Managements** (kurz: MDM, zu deutsch: Mobilgeräteverwaltung) werden alle Geräte eines Unternehmens durch eine Software zentral gewartet und verwaltet.

DIGITAL SICHER NRW

WIE SICH MOBILE GERÄTE SICHER VERWALTEN LASSEN: DAS MOBILE DEVICE MANAGEMENT

DER EINSATZ EINES MDM IST SINNVOLL, WENN…

- Mobilgeräte innerhalb des Unternehmens im Einsatz sind,
- ein hoher Sicherheitsbedarf besteht und Ressourcen für Konfigurations- und Verwaltungsaufwand verfügbar sind.

BEI DER BETRIEBLICHEN NUTZUNG PRIVATER GERÄTE…

- muss das Einverständnis eingeholt werden, dass der Arbeitgeber das private Gerät verwalten bzw. kontrollieren darf.

Dies ist mit Blick auf den Datenschutz und die Mitarbeiterakzeptanz nicht immer einfach.
Eine mögliche Alternative ist die „Container-Lösung“.

DIGITAL SICHER NRW

WIE SICH MOBILE GERÄTE SICHER VERWALTEN LASSEN: DIE “CONTAINER-LÖSUNG”

DIE “CONTAINER-LÖSUNG” IST SINNVOLL, WENN…

- Privatgeräte betrieblich genutzt werden (“Bring your own Device“),
- die zur Verfügung gestellten mobilen Geräte von Mitarbeitenden auch privat genutzt werden dürfen.

BEI DER ”CONTAINER-LÖSUNG”…

- ist der Container mit einer eigenen Authentifizierung abgesichert,
- werden Unternehmensdaten verschlüsselt in sogenannten Containern gespeichert,
- muss das Gerät nicht speziell modifiziert werden,
- ist der Schutz der Privatsphäre der Mitarbeitenden gewährleistet,
- gibt es einen geringeren Administrationsaufwand gegenüber dem Mobile Device Management.

CHANCEN UND HERAUSFORDERUNGEN VON “BRING YOUR OWN DEVICE”

DIGITAL SICHER NRW

VORTEILE VON “BRING YOUR OWN DEVICE”

- Die Flexibilität und Mobilität der Mitarbeitenden wird gesteigert,
- es wird eine größere Auswahl an Gerätetypen ermöglicht,
- die Kosten für Hard- und Software werden gesenkt.

NACHTEILE VON “BRING YOUR OWN DEVICE”

- Das Unternehmen hat keine oder eine eingeschränkte Kontrolle über Geräte,
- die Sicherheit und DSGVO-Konformität der Firmen-Daten ist nur eingeschränkt gewährleistet,
- das Risiko für Datenlecks ist höher,
- die Geräte- und App-Sicherheit ist ggfs. nicht gegeben.

SICHERE VERWALTUNG MOBILER GERÄTE: EIN MUSS FÜR JEDES UNTERNEHMEN!

Smartphones und Tablets sind zum Dreh- und Angelpunkt unserer alltäglichen Kommunikation geworden – das gilt auch für den beruflichen Alltag. Auf ihnen werden persönliche Dokumente gespeichert und sie sind oft mit sensiblen Bereichen wie Bankkonten und Aktiendepots verknüpft.
Nehmen Sie deshalb in Ihrem Unternehmen jetzt die entsprechenden Maßnahmen vor und seien Sie für den Ernstfall eines Diebstahls oder eines Verlusts gewappnet!

Sie haben weitere Fragen zum sicheren Einsatz mobiler Geräte in Ihrem Unternehmen?
Dann besuchen Sie gerne unsere digitalen Sprechstunde oder melden Sie sich für unsere Erstberatung an.
Zur Anmeldung gelangen Sie über unsere Webseite.

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

Weitere Informationen finden Sie unter **www.digital-sicher.nrw**.