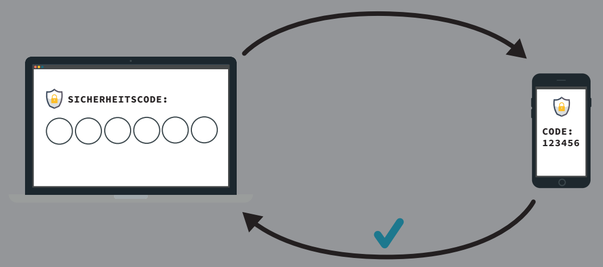
SECURITY IN DER CLOUD

Viele bringen das Wort Cloud auch heute noch mit unbekannten Risiken in Verbindung. Die Microsoft Cloud ist hingegen vielfach geprüft, hunderte Mitarbeiter kümmern sich jeden Tag um die Sicherheit dieser Cloud und das Schließen von möglichen Sicherheitslücken. Viele Unternehmen kommen deshalb inzwischen zu dem Schluss, dass die Datenablage in der Cloud sogar sicherer ist, als deren bisherige Speicherung auf eigenen Serverfarmen. Neben dem, was Microsoft für die Sicherheit eurer Daten tut, könnt ihr mit folgenden Einstellungen zusätzlich selbst das Risiko verringern:

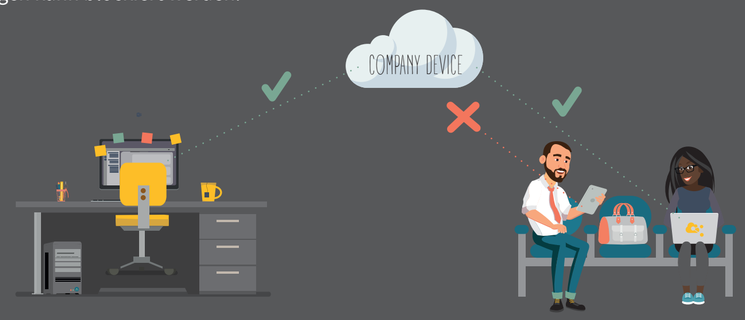
ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Es ist möglich eine Zwei-Faktor-Authentifizierung einzustellen. Damit ist die Anmeldung für Office365 User nur mit zwei Devices möglich. Das heißt, neben der Abfrage von User und Passwort, wird auf ein weiteres Gerät ein Code geschickt. Ohne diesen Code ist eine Anmeldung nicht möglich. Diese Sicherheitseinstellung schwächt die Gefahr durch leichte Passwörter.



ZUGRIFF NICHT VERWALTETER GERÄTE STEUERN

Für nicht verwaltete Geräte (die nicht mit einer Domäne verbunden oder in Intune* kompatibel sind) kann der Zugriff blockiert oder eingeschränkt werden. So können User nicht verwalteter Geräte z.B. keine Dateien herunterladen, drucken oder synchronisieren. Selbst Screenshots zu erzeugen kann blockiert werden.



* Intune ist ein cloudbasierter Dienst, über den Geräte wie Laptops, Handys usw. – die für den Zugriff auf Unternehmensdaten genutzt werden – verwaltet werden. Hier können für die Geräte Sicherheitseinstellungen, wie z.B. Passwort Anforderungen, vorgenommen werden.

UND DAS KANNST DU SELBST ZUR SICHERHEIT BEITRAGEN

PASSWÖRTER

Um selbst zur Sicherheit beizutragen ist es wichtig, dass Passwörter nie aufgeschrieben und regelmäßig geändert werden. Außerdem ist es sinnvoll, auch wenn es nicht unbedingt vorgeben ist, Passwörter mit Zahlen, Buchstaben und Sonderzeichen zu versehen.

BEKANNTE CLOUD SERVICES

Bitte nutzt nur die Dienste, die für euer Unternehmen genehmigt sind. Fragt in der IT-Abteilung nach, welche das sind. Zu schnell werden Nachrichten mit wichtigen Daten über ungesicherte Cloud Dienste verschickt.

FREMDE AUGEN UND OHREN

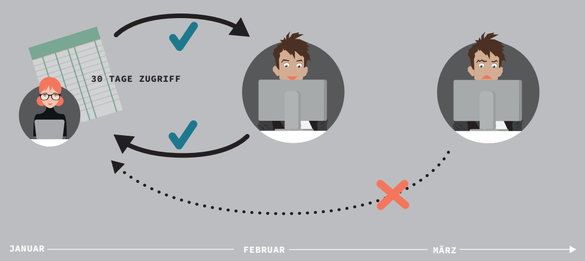
Sperrt euren Bildschirm wenn ihr von eurem Arbeitsplatz aufsteht. Aber vorallem auch außerhalb des Firmengeländes sollte das mobile Endgerät unbedingt vor unbefugter Nutzung geschützt werden. Schaut auch an Flughäfen oder im Zug wer mithört- oder sieht.

INAKTIVE USER ABMELDEN

User, die eine festgelegte Zeitspanne inaktiv waren, werden automatisch abgemeldet. Das Risiko eines Zugriffs durch unbefugte Dritte wird so minimiert.

TEILEN, ABER MIT VORSICHT

Wenn Inhalte geteilt werden, verwendet Links die ablaufen oder nur eingeschränkte Rechte gewähren. Bei eingeladenen Gästen, zum Beispiel in Teams, muss bei Beendigung der Zusammenarbeit der Zugriff wieder entfernt bzw. die Berechtigung auf anderweitig geteilte Dateien angepasst werden.



ZUGRIFF ÜBER NETZWERKSTANDORT STEUERN

Es ist möglich eine vertrauenswürdige Netzwerkumgebung zu definieren und eine Netzwerkgrenze festzulegen. Ein Nutzer außerhalb dieser Netzwerkgrenze erhält keinen Zugriff auf die Daten. Zusätzlich können IP-Adressen einzeln hinzugefügt werden und gelten dann als vertrauenswürdig.

© www.nuboworkers.com