BRING YOUR OWN DEVICE: DOS AND DON'TS

Bei der IT-Sicherheit müssen Geschäftsführung, IT-Administrator und Mitarbeiter an einem Strang ziehen.

Rechtens, sicher und komfortabel

Das Thema IT-Sicherheit gewinnt in Unternehmen nicht zuletzt durch das Inkrafttreten der Datenschutzgrundverordnung (DSGVO) zunehmend Bedeutung. Darf ich mein privates Tablet im Firmennetzwerk nutzen? Und welcher Internetbrowser ist wirklich sicher? Wenn alle drängenden Fragen zur Zufriedenheit aller und des Datenschutzbeauftragten beantwortet sein sollen, müssen alle an einem Strang ziehen: Geschäftsführung, IT-Administrator und Mitarbeiter.

Ob im Büro, im Außendienst oder zu Hause im Homeoffice: Private Mobilgeräte auch für Dienstzwecke nutzen zu können, hat sich als i-Tüpfelchen einer komfortablen Arbeitsorganisation etabliert. Das Mantra lautet: Bring Your Own Device (BYOD). Um generell einen sicheren und gleichermaßen produktiven Einsatz von Smartphones, Tablets, Laptops, Convertibles und Co. zu forcieren, steht die Unternehmensleitung in der Pflicht, ein sogenanntes Enterprise-Mobility-Management (EMM) zu etablieren.

IT-Sicherheitslotse Pierre Gronau

So eine Strategie beschäftigt sich nicht nur mit Sicherheitsfragen, sondern unterstützt Mitarbeiter auch bei ihrer täglichen Arbeit, indem sie Klarheit für alle Beteiligte schafft. Sie gibt jedem im Unternehmen Hilfestellung, wenn es darum geht, arbeitsbezogene Aufgaben auf Mobilgeräten durchzuführen. Ein sinnvolles unternehmensinternes BYOD-Programm hält technische und organisatorische Voraussetzungen fest, um private Geräte für die dienstliche Nutzung zu erlauben. Wichtig ist, dass Unternehmen die Einhaltung dieser Anforderungen regelmäßig kontrollieren.

ÜBERBLICK FÜR DEN IT-VERANTWORTLICHEN IM UNTERNEHMEN

Wie dies umgesetzt werden kann, illustriert Pierre Gronau, Gründer der Berliner Gronau IT Cloud Computing GmbH. Ein mit dem Sicherheitsthema betrauter IT-Mitarbeiter sollte den Einsatz mobiler Geräte der Kollegen, wie zum Beispiel Smartphones und Tablets, überblicken und zentral administrieren und überwachen. Dabei spielt es keine Rolle, ob die mobilen Geräte vom Unternehmen angeschafft wurden oder sich im Privatbesitz der oder des Mitarbeitenden befinden – alle Geräte sollten zwingend an zentraler Stelle angemeldet sein und der entsprechende Mitarbeiter sollte die Konfiguration alleinig verantworten. Überschaubar bleiben diese Prozesse, wenn der Zuständige jedes Gerät über ein sogenanntes Mobile-Device-Management, eine Web-Konsole, löschen, konfigurieren und sperren kann sowie ihre Einstellungen hierüber kontinuierlich kontrolliert. Über eine Integration spezieller Tools in die vorhandenen IT-Strukturen kann es zudem gelingen, die Einhaltung firmeneigener Sicherheitsmaßgaben sowie einen sicheren Zugang zum Firmennetz zu gewährleisten, Verschlüsselungen vorzunehmen und Anwendungen zu verwalten.

ACHTUNG, HACKER!

IT-Berater Gronau empfiehlt, Zeitserver und Zeitzonen auf „Automatisch einstellen" zu konfigurieren, um Unregelmäßigkeiten und Angriffe auf das System zeitlich exakt analysieren zu können. Zudem sollten IT-Administratoren Mindestanforderungen an eine sichere und datenschutzkonforme Konfiguration von Webbrowsern anwenden. Alle Massenspeicher wie Festplatten und Flash-Speicher sollten mit aktueller Kryptografie-Technik verschlüsselt sein – unabhängig, ob es sich um interne oder externe Speichermedien handelt.

Der Einsatz mobiler Devices im Unternehmen bedarf Sicherheitsvorkehrungen.

Gute Passwort-Politik als Basis für den Datenschutz

Parallel sollten sensible Daten und Firmeninterna in abstreitbarer Form, beispielsweise in einen VeraCrypt-Container abgespeichert werden. Cloudbasierte Passwort-Management-Dienste sind nicht empfehlenswert.

Administratoren sollten von den jeweiligen Herstellern angebotene Software-Aktualisierungen ohne Zeitverzug einspielen, mindestens jedoch monatlich. Dafür ist es ratsam, die Software-Aktualisierungsfunktion auf „Automatisch" einzustellen. Bei Software aus App-Stores müssen IT-Mitarbeiter und Anwender sicherstellen, dass ausschließlich vom Hersteller und vom Unternehmen angebotene und freigegebene Software zum Einsatz kommt. Ist zudem eine lokale Firewall verfügbar, so sollte sie aktiviert und alle Geräte sollten mit einem Malware-Schutz ausgestattet sein. Dieser ist idealerweise auf stündliche automatische Aktualisierung konfiguriert. Alle Geräte sollten so eingestellt sein, dass die Übermittlung von personenbezogenen Daten gemäß EU-DSGVO an die Hersteller unterbunden oder zumindest minimiert

wird. Bei Vorhaltung besonders schützenswerter Daten wie elektronische Personalakten müssen unternehmensspezifische weitergehende Maßnahmen greifen.

DER AUFGEKLÄRTE ANWENDER

Voraussetzung ist die Einbeziehung von Anwendern, um wirkungsvolle, angemessene, sichere und vertrauenswürdige IT-Lösungen zu schaffen.

Laptops sollten auch unterwegs gut geschützt sein.

Experte Gronau empfiehlt daher Unternehmen, ihren Mitarbeitern, denen sie mobilen ITK-Geräte wie Smartphones, Tablets und Laptops aushändigen, hiermit klar verbundene IT-Sicherheitshinweise an die Hand zu geben und eine Dienstvereinbarung unterschreiben zu lassen. Ebenso kann eine Betriebsvereinbarung sinnvoll und angezeigt sein. Bei Diebstahl der Geräte sollten Mitarbeiter dies unverzüglich der Polizei mitteilen und eine vorher festgelegte Abteilung darüber informieren. Letztere muss auch bei Beschädigung der Geräte unverzüglich informiert werden. Um den Zugriff unbefugter Dritter zu verhindern, sollten die Geräte nicht unbeaufsichtigt und offen sichtbar in Betriebsräumen, Hotelzimmern oder Fahrzeugen liegen. Integrierte Kameras gilt es mit einem zusätzlichen physischen Schutz auszustatten und vorhandene Sicherheitsfunktionen der Geräte zu nutzen.

Gerätenutzer sollten auf Reisen, dies gilt insbesondere für Tablets, Convertibles und Laptops, Blickschutzfilter nutzen, die das Mitlesen Dritter verhindern, indem sie die Blickwinkel stark beschränken. Auf Flügen ist es erste Wahl, Mobile Devices im dafür geeigneten Handgepäck mitzuführen. Inzwischen ist ein Mitführen von Tablets und Laptops im Handgepäck bei manchen Flügen untersagt. Dann verstauen Mitarbeiter die technische Ausstattung in einem geeigneten Transportbehältnis, womit keine handelsüblichen Notebooktaschen gemeint sind. Das elektronische Kennzeichnen von Reisegepäck mithilfe von beispielsweise RFID oder Bluetooth sollte Anwendern ebenso untersagt sein wie die Nutzung fremder, nicht autorisierter Ladestationen.

Es ergibt Sinn, dass Anwender regelmäßig, heißt hier mindestens wöchentlich, eine Datensicherung durchführen. Unabhängig davon empfiehlt sich, dass jeder Mitarbeiter ausschließlich mit unternehmensinternen Daten umgeht, wenn er sich in einer sicheren, vom Arbeitgeber betriebenen Netzinfrastruktur bewegt: Außerhalb dieser ist das Arbeiten an und mit dienstlichen Daten und Anwendungen nur dann akzeptabel, wenn eine gesicherte Verbindung zur Netzinfrastruktur der Firma besteht (z. B. durch einen gesicherten VPN-Tunnel) oder alle Datenverbindungen von Smartphone, Tablet und Co. zuvor unterbrochen wurden, wie dies im „Flugmodus“ der Fall ist. Bei der Nutzung von E-Mails sollten Mitarbeiter die von der Firma zur Verfügung gestellten E-Mail-Filterfunktionen wie Positiv-Liste (Whitelists), Negativ-Liste (Blacklists) und Bayes-basierte Spamfilter nutzen und E-Mails nur verschlüsselt senden und empfangen.

Allen oben aufgeführten Punkte setzen voraus, dass jeder Mitarbeiter, der im und für sein Unternehmen mit mobilen Geräten arbeitet, geschult und über datenspezifische Risiken aufgeklärt wird. Klare Compliance-Richtlinien und Kommunikations- sowie Entscheidungswege bilden die Basis dafür, dass sich EEM-Konzepte in gelebten Digitalalltag wandeln.

FÜNF INTERNET-TO-DOS ALS SICHERHEITSGUIDE

Die nachfolgenden Handlungsempfehlungen bilden ein solides Gerüst für den Internet-Part firmeninterner IT-Sicherheitskonzepte.

1. Browserwahl
Bei der Nutzung von Webseiten der Firma sollte ein anderer Internetbrowser verwendet werden und in besonders unsicheren, kritischen Umgebungen bietet sich der „Tor Browser“ für anonymes „Surfen“ an. Ein aktivierter Pop-up-Blocker sowie ein Phishing-Filter gehören an dieser Stelle ebenso zum sicherheitsrelevanten Standard.

2. Vertrauenswürdige Kommunikation
Um die vertrauenswürdige Kommunikation mithilfe von Zertifikaten zu erreichen, muss eine angemessene Prüfung der Zertifikatskette erfolgen. Die Voreinstellung „Do Not Track“ im Webbrowser hilft gegen unnötige Datenerhebung. Ebenso sollten Mitarbeiter keine Zugangsdaten und Passwörter speichern.

3. Klarheit für den Nutzer
Passende Webbrowser zeichnen sich dadurch aus, dass sie für das Unternehmensumfeld geeignet und nicht manipulierbar sind. Sie zeigen ihren Nutzern zum Beispiel durch Farbe oder Symbole an, ob die Kommunikation mit dem Webserver verschlüsselt oder unverschlüsselt erfolgt. Ein fehlendes Zertifikat im Speicher oder ein ungültiges respektive widerrufenes Server-Zertifikat als Prüfergebnis muss signalisiert werden und eine verschlüsselte Verbindung sich in solch einem Fall ausschließlich nach ausdrücklicher Bestätigung durch den Nutzer aufbauen.

4. Integritätsprüfungen der Updates
Es empfiehlt sich, Updates nur dann einzuspielen, wenn die Integritätsprüfung erfolgreich war. Fehlerhafte Prüfergebnisse hingegen sollten dem Anwender angezeigt werden und das Update ist dann folgerichtig tabu. Die Voreinstellung „Do Not Track“ im Webbrowser ergibt Sinn.

5. Suchmaschinen
Administratoren sollten folgende datenschutzkonforme Suchmaschinen auf den Browsern voreinstellen und zur Nutzung freigeben:

- **Metager:** metager.de
- **Startpage:** www.startpage.com
- **Qwant:** www.qwant.com
- **DuckDuckGo:** duckduckgo.com