WEB +APP
Besser surfen, mehr erleben

Von **Valerie Hagmann**

...aber sicher!

HOME-OFFICE:

Datenverlust vorbeugen

Die Corona-Pandemie hat unseren Alltag verändert. Wer auf Telearbeit umstellen musste, sollte sich folgende Tipps zu Herzen nehmen, damit wichtige Dokumente und Dateien nicht verloren gehen.

Die derzeitige Ausbreitung des Coronavirus hat den Arbeitsplatz vieler Menschen schlagartig ins Home-Office verlegt, was für die meisten eine große Umstellung darstellt. Arbeitsabläufe und die Zusammenarbeit in Teams werden vor neue Herausforderungen gestellt. Hinzu kommt, dass bei Heimarbeit die Gefahr von Datenverlust steigt – und leider auch Cyber-Betrüger vermehrt die Gunst der Stunde nutzen.

e-media hat für Sie die wichtigsten Tipps zusammengestellt, die es zu beachten gilt, damit auch beim Arbeiten im heimischen Büro persönliche und arbeitsrelevante Daten sicher sind.

Software aktuell halten

Grundsätzlich ist es nicht nur im Arbeitskontext sinnvoll, wichtige Software möglichst auf dem neuesten Stand zu halten. Um den PC zu schützen, sollte deshalb zuallererst das Betriebssystem auf Aktualität überprüft werden. Ob Updates vorliegen, lässt sich im Windows Update Center feststellen. Dazu in den Einstellungen Windows Update öffnen und gegebenenfalls ausstehende Updates herunterladen und installieren.

Abgesehen vom Betriebssystem sollten Sie auch alle anderen Programme, mit denen Sie arbeiten, in ihrer aktuellsten Version verwenden. Das gilt natürlich genauso für das Smartphone, vor allem wenn es im beruflichen Kontext verwendet wird.

Besonders wichtig: Wenn Sie zusätzliche Apps und Programme herunterladen, achten Sie auf vertrauenswürdige Quellen (offizielle App-Stores bzw. Portale der jeweiligen Hersteller) oder beschränken Sie sich auf die vom Arbeitgeber bereitgestellte Software.

Malware & Hacker aussperren

Als Nächstes gilt es, sich um ordentlichen Schutz vor Schadsoftware zu kümmern. Unter Windows 10 bietet der hauseigene Windows Defender grundlegenden Schutz. Eine Installation ist nicht notwendig, die Software ist im Betriebssystem integriert und wird mit jeder Aktualisierung desselben auf den neuesten Stand gebracht. Zusätzlich sollte unbedingt die Windows Firewall aktiviert werden, so noch nicht passiert. Dafür in der Suchleiste am Windows-Desktop links unten „Windows Defender Firewall" suchen und in den Einstellungen einschalten.

Weil aber gegen die immer komplexere Malware Basisschutz oft nicht ausreicht, empfehlen wir den Einsatz von Internet-Security-Lösungen. Ein solches Schutzpaket muss nicht unbedingt gleich gekauft werden. Auf den Portalen aller namhaften Hersteller (etwa *eset.com/at, gdata.at, kaspersky.at* ...) gibt es

im Downloadbereich kostenlose 30-tägige Testversionen der Security-Pakete – und zwar in vollem Funktionsumfang. Von Gratis-Schutzprogrammen raten wir hingegen ab – schließlich ist der Windows Defender schon vorinstalliert.

VPN verwenden

Ein Virtual Private Network, kurz VPN, sollte für das Home-Office unbedingt eingerichtet werden, schon um sicher zu kommunizieren. Ein VPN-Zugang wird auch verwendet, um von außerhalb auf Firmenserver zugreifen zu können. Das VPN erstellt eine verschlüsselte Verbindung, eine Art Tunnel, der sämtliche Netzwerkaktivitäten vor unerwünschtem Zugriff schützt. Nutzungsdaten werden hierbei verschleiert. In der Regel wird ein VPN-Zugang vom Unternehmen ausgegeben. Hat man die Möglichkeit, über ein VPN im Firmennetzwerk zu arbeiten, sollte man diese auch nutzen, um Daten direkt am Firmenserver abzulegen. In Firmennetzwerken werden sämtliche Dateien im Normalfall regelmäßig gesichert.

Doch auch für den Privatgebrauch kann ein VPN-Zugang nützlich sein, dafür gibt es zahlreiche Anbieter. Allerdings: Finger weg von kostenlosen Angeboten, denn sie haben nachgewiesenermaßen oft einen Haken und geben erst recht Nutzerdaten weiter, um sich zu finanzieren. Zu den empfehlenswerten VPN-Diensten mit gutem Preis-Leistungs-Verhältnis zählen zum Beispiel NordVPN, CyberGhost, PureVPN oder ProtonVPN.

Passwörter auffrischen

Egal, ob privat oder beruflich, adäquate Passwörter für E-Mail-Clients, Messenger-Dienste und andere arbeitsrelevante Programme sollten ernst genommen werden. Beim Arbeiten im Home-Office gilt das nicht nur für Website-Login-Daten, sondern auch für das heimische WLAN. Viele verwenden das vom Provider voreingestellte Passwort, das direkt am WLAN-Router aufgeklebt ist. Sicherer ist es, das Passwort zu ändern. Der Vorgang unterscheidet sich von Hersteller zu Hersteller. Infos dazu gibt es auf der Website Ihres Internet-Providers bzw. im Router-Handbuch.

Zur Erinnerung: Ein gutes Passwort ist im Idealfall eine möglichst sinnfreie Kombination aus Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen mit einer Länge von mindestens acht Zeichen. Spätestens jetzt ist ein guter Zeitpunkt, um lange verstaubte Passwörter wieder einmal zu ändern und zu verbessern. Damit man den Überblick nicht verliert, kann ein Passwortmanager Abhilfe schaffen, zum Beispiel 1Password, Bitwarden oder Keepass.

Extratipp: Nutzen Sie für Login-Vorgänge die Zwei-Wege-Authentifizierung, wo immer das möglich ist. Mit dieser Methode muss neben Benutzername und Passwort zusätzlich ein Einmalcode eingegeben werden, der gesondert ans Smartphone geschickt wird.

Backup-Tools nutzen

Generell empfiehlt es sich, Daten extern zu sichern, vor allem wenn Dateien nicht direkt über einen VPN-Zugang am Firmenserver abgelegt werden können. Neben der PC-Festplatte sollten besonders wichtige Dokumente und Daten grundsätzlich auf einem externen Speichermedium, also USB-Stick oder externer Festplatte, abgespeichert werden, denn Hardware kann kaputtgehen. In einigen Fällen ist es auch praktisch, Dateien in der Cloud zwischenzulagern. Bei besonders heiklen Daten sollte der Cloud-Dienst mit Bedacht ausgewählt werden.

Daten verschlüsseln

Wer sensible Dokumente und Dateien auf der Festplatte hat, sollte die Hardware unbedingt verschlüsseln. Das garantiert, dass nur autorisierte Personen Zugriff auf heikle Daten haben. Dies gilt auch für Files, die in die Cloud geladen werden. Die Pro-Version von Windows 10 hat mit BitLocker hierfür bereits eine Lösung an Bord. BitLocker muss über die Systemsteuerung aktiviert werden, danach lässt es sich mit einem Rechtsklick auf das jeweilige Laufwerk starten. Für den Zugriff auf das Laufwerk ist danach ein Passwort nötig.

Sollen nicht gleich ganze Laufwerke verschlüsselt werden, sind externe Tools eine gute Lösung, etwa die Software VeraCrypt. Sie kann einzelne Dateien vor Fremdzugriff schützen.

In der Cloud arbeiten

Für die Zusammenarbeit mit Kollegen bei räumlicher Trennung bieten sich Cloud-Dienste an. Auf Daten kann jederzeit von überall aus zugegriffen werden, Inhalte können geteilt, Projekte auch über weite Distanzen hinweg organisiert und von mehreren Personen bearbeitet werden. Das bedeutet allerdings auch, dass private Daten einem externen Anbieter anvertraut werden. Die Server gängiger Cloud-Anbieter stehen oft in Asien oder den USA und sind rechtlich damit schwer greifbar. Als Alternative zum beliebten Google Drive gibt es inzwischen mehrere Dienste mit Servern auf österreichischem Boden, womit sie europäischen Datenschutzgesetzen unterliegen. Ein solcher Anbieter ist die Plattform Cloudinho, die wir in Ausgabe 03/2020 vorgestellt haben.

Extratipp: *e-media* verlost in dieser Ausgabe 20 Jahrespakete mit je 30 GB Speicherplatz bei Cloudinho. Mehr dazu auf Seite 21!

Vorsicht: Phishing

Betrügerische E-Mails und manipulierte Websites haben derzeit Hochsaison. Suchen Sie in Krisenzeiten Informationen zur aktuellen Lage, ist Wachsamkeit geboten. Betrüger nutzen die Situation vermehrt, um Ihre Daten abzugreifen. Der einschlägige Spam macht auch vor dem Arbeitspostfach nicht halt. Werden Sie per Mail aufgefordert, neue Software für die Heimarbeit zu installieren oder ihre Zugangsdaten für ein Kollaborationstool einzugeben, um dieses zu aktivieren, seien Sie skeptisch. Kontrollieren Sie den Absender genau und fragen Sie im Zweifelsfall telefonisch bei Kollegen oder der IT-Abteilung nach.

Derzeit kursieren auch E-Mails, in denen aktuelle Informationen und Verhaltenstipps zur Pandemie versprochen werden. Hinter dem eingefügten Download-Link verbirgt sich jedoch Schadsoftware. Generell gilt: Öffnen Sie keine E-Mails oder Anhänge unbekannter Herkunft. Klicken Sie auch nicht auf Links zu vermeintlich bekannten Websites im E-Mail. Ist die Schreibweise nur geringfügig anders, geht man ein Sicherheitsrisiko ein – daher die Web-Adresse besser immer händisch eintippen. <<

FOTO: SHUTTERSTOCK