Cyberkriminalität: Im Urlaub auf Nummer sicher gehen

(ots)

Auf Reisen sind Mobilgeräte wie Smartphone, Tablet oder Notebook unverzichtbare Begleiter geworden. Laut einer Umfrage des Digitalverbandes Bitkom nehmen 76 Prozent der Deutschen ihr Smartphone mit in den Urlaub. Gerade durch die Corona-Pandemie haben die mobilen Geräte noch mehr an Relevanz gewonnen. Deswegen wollen Cyberkriminelle derzeit nicht nur von der Unbedarftheit der Anwender im Urlaub profitieren, sondern auch von der aktuellen Krisensituation. Mit gefälschten und schadhaften Corona-Apps versuchen sie, das Informationsbedürfnis und das Interesse an Warn-Apps auszunutzen. Auch das Teilen von Schnappschüssen und Erlebnissen in den sozialen Medien, kann Reisenden schnell zum Verhängnis werden. So erhalten Kriminelle über Facebook, Instagram und Co. schnell Einblick, wer sich nicht Zuhause aufhält. An den Urlaubsorten versuchen Datendiebe mit manipulierten, öffentlichen WLAN-Netzen sensible Daten wie Kreditkarteninformationen zu stehlen. ESET empfiehlt Reisenden schon vor dem Urlaubsbeginn, ihre mobilen Begleiter umfassend abzusichern und gibt Tipps, was vor Ort zu beherzigen ist.

„Gerade im Ausland sind öffentliche WiFi-Hotspots in Restaurants, Hotels und Bars bei Urlaubern sehr beliebt. Deswegen sind hier Cyberkriminelle sehr aktiv, um sensible Daten zu erbeuten“, erklärt Thomas Uhlemann, ESET Security Specialist. „Reisende können die WLAN-Angebote nutzen, sollten

aber niemals vertrauliche Daten wie Kreditkarteninformationen preisgeben und auch keine Online-Bankgeschäfte oder ähnliches tätigen.“

Vorsicht vor gefälschten Corona-Apps

Cyberkriminelle nutzen seit Monaten die Corona-Pandemie für ihre Zwecke aus -auch im Urlaub. Mithilfe der Corona-Warn-Apps, die in vielen Ländern bereits verfügbar sind, können Begegnungen zwischen den Nutzern der App nachvollzogen werden. Ziel ist es, die Menschen, die in Kontakt mit positiv getesteten Personen standen, zu alarmieren. Kriminelle versuchen daraus Kapital zu schlagen, indem sie gefälschte Apps in den Stores platzieren. Gerade im Ausland sollten Urlauber hier Vorsicht walten lassen und nicht auf manipulierte Warn-Apps hereinfallen. In Zukunft sollen die Anwendungen in den europäischen Ländern untereinander kompatibel werden.

Vermeintliche WiFi-Angeboten genau prüfen

Egal ob in der Berghütte, dem Strandbungalow, auf dem Campingplatz oder im Hotel: Die meisten Menschen suchen im Urlaub Erholung, ohne auf das Internet verzichten zu müssen. Das wissen auch Cyberkriminelle und haben speziell präparierte Hotspots in den Urlaubsregionen im Einsatz. Müssen Urlauber sensible Daten, wie Kreditkarteninformationen oder Facebook-Zugangsdaten für die Nutzung des kostenlosen WLANs eingeben, sollten sie das Angebot keinesfalls nutzen! Die Gefahr, hier auf Betrüger hereinzufallen, ist sehr hoch. Bei der Nutzung kostenloser WLAN-Hotspots sollte zudem immer eine VPN-Lösung zum Einsatz kommen. Die Technologie schützt den eigenen Datenverkehr vor neugierigen Blicken.

Datensparsamkeit in sozialen Netzwerken

Jeder Zweite teilt seine Reiseerlebnisse in den sozialen Medien oder einem Blog. Zu diesem Ergebnis kommt der Digitalverband Bitkom in einer aktuellen Umfrage. So reizvoll

es auch sein mag, den Schnappschuss im Sonnenuntergang seinen Freunden oder Verwandten zuhause zu zeigen: Das Teilen der Urlaubsfotos in sozialen Netzwerken wie Facebook oder Instagram sollte auf die Zeit nach der Rückkehr verschoben werden. Das Risiko ist groß, Einbruchsopfer zu werden, wenn Fremde durch Postings erfahren, dass Haus oder Wohnung leer stehen.

Tipps für einen sicheren Urlaub

- Anti-Diebstahl-Lösungen einsetzen: Im Urlaub gehen Smartphones, Tablets und Notebooks leichter verloren. Damit es Langfinger schwer haben, nutzen moderne Anti-Diebstahl-Module, wie in den ESET Sicherheitslöungen enthalten, zum Beispiel die eingebaute Kamera, um den Täter unbemerkt zu fotografieren. Zudem lokalisieren sie die Geo-Koordinaten des verlorenen Geräts.
- Wichtige Daten sichern: Wichtige Daten auf dem Smartphone und Tablet können mit einem Backup gesichert werden. Dazu bieten sich USB-Sticks, externe Festplaten oder Cloud-Dienste an. Bei Verlust der Hardware sind so zumindest die Daten nicht verloren und lassen sich später wiederherstellen.
- Keine Corona-Warn-Apps aus dem Ausland herunterladen: Cyberkriminelle wollen mit gefälschten und schädlichen Corona-Warn-Apps Profit erzielen. Gerade Touristen im Ausland suchen derzeit in den App-Stores nach solchen Angeboten . Hier sollten Nutzer deshalb besser warten, bis die Corona-Warn-App mit den Anwendungen anderer Länder kompatibel ist. Bis dahin gilt: Eine App kann nur warnen, Mund-Nasenschutz und Abstand schützen.
- Software und Sicherheitslösungen aktualisieren: Das Betriebssystem, die installierten Apps und die verwendeten Sicherheitslösungen sollten auf dem neuesten Stand sein. Das verhindert das Ausnutzen bekannter Sicherheitslücken.
- Sicherheitssoftware installieren: Auf dem Smartphone, Tablet oder Notebook sollten Anwender eine Security-Software installieren. Neben einem zuverlässigen Schutz vor Malware und anderen Bedrohungen sind Sicherheitslösungen empfehlenswert, die zudem Funktionen wie Diebstahl-Schutz beinhalten.
- WiFi-Hotspots nur mit VPN-Verbindung nutzen: Hotels, Bars und andere Locations locken Urlauber mit kostenlosem WiFi-

Zugang. Gerade bei Fernreisen ist das praktisch, weil Urlauber häufig keine zusätzliche SIM-Karten besitzen und das eigene Datenvolumen begrenzt ist. Über ein solches Netzwerk besteht aber die Gefahr, dass Kriminelle sensible Daten oder wichtige Daten wie Login- oder Kreditkartendaten ausspähen. Anwender sollten daher die Verbindung zusätzlich mit einer vertrauenswürdigen VPN-Lösung sichern. Einkäufe oder Finanzgeschäfte sollten aber dennoch auf die Zeit nach dem Urlaub verschoben werden.

- Posting in sozialen Medien: Um virtuellen und realen Dieben die Vorbereitung für einen Einbruch nicht zu vereinfachen, sollten Anwender in den sozialen Medien nichts über ihren Urlaub posten.
- Vorsicht beim Bezahlen: Kontaktloses Bezahlen ist auch in den Urlaubsorten immer häufiger möglich. Eine spezielle Schutzhülle oder ein Portemonnaie schirmt die Kredit- oder EC-Karten ab. So können Diebe die Daten nicht mit speziellen Geräten auslesen. Alternativ können je nach Unterstützung durch die Hausbank auch Apple oder Google Pay genutzt werden. Das erhöht die Sicherheit beim Bezahlvorgang.
- Funknetze deaktivieren: Werden sie nicht benötigt, können die Bluetooth- und WLAN-Funktionen deaktiviert werden. Dadurch verringern Nutzer die möglichen Angriffsflächen für Cyberkriminelle

Original-Content von: ESET Deutschland GmbH,