Sommer, Sonne, Cyberfrust?

In Zeiten, in denen sich die Nutzung privater und geschäftlicher Mobilgeräte immer mehr vermischt, ist besondere Vorsicht vor Cyberattacken geboten. Im Urlaubsglück vernachlässigte Sicherheitsregeln werden schnell zum Fiasko – im Privaten ebenso wie im Geschäftlichen.

Urlaub kommt genau wie Weihnachten immer plötzlich – ergo rasch den Koffer gepackt, die unverzichtbaren digitalen Geräte eingesteckt und los geht's in die Ferien. Notebooks, Tablets und Smartphones ohne aktuelle Updates, unsichere Zugänge zu Benutzerkonten und das arglose Nutzen der Geräte an Strand, Pool und Sehenswürdigkeiten sind Top-Chancen für die Cyberkriminellen. Sie wissen genau, wie leicht sie in der Urlaubszeit an persönliche Daten, User-Konten oder andere wertvolle Informationen kommen. Das Brisante daran ist, dass immer mehr Geräte sowohl für Privates als auch berufliche Zwecke verwendet werden – ein gefundenes Fressen für Hacker und eine potenzielle Katastrophe für private und geschäftliche Daten.

Um diese Risiken zu reduzieren ist es wichtig, Wachsamkeit und natürlich auch den gesunden Menschenverstand nicht zuhause zu lassen und vor allem Geräte und Konten bereits vor Antritt der Reise auf Aktualität und Sicherheit zu prüfen. Sichere Passwörter oder ein Passwortmanager, Zwei-Faktor-Authentifizierung und eine wirkungsvolle Schutzsoftware sollten auf jeden Fall mit auf Reisen gehen. Wer es sich einfach machen möchte, kann auf die vielen kostenlosen Sicherheits-Tools renommierter Security-Anbieter zurückgreifen. Zudem gilt (auch) auf Reisen: auffallend preiswerte Angebote oder komische Einladungen per E-Mail, SMS oder via Sozialen Medien ignorieren.

Sophos hat es für Reisende leicht gemacht und fünf Tipps zusammengestellt:

1) Gerätesicherheit noch vor der Reise
Wo viele Touristen sind, lauern die Ganoven. Denn Geräte und Apps ohne oder mit schlechten Passwörtern sowohl beim Klau der Devices als auch im digitalen Raum zum Problem. Am besten ist es daher, nur Geräte mitzunehmen, die man wirklich benötigt. Zudem sollten alle Reisebegleiter sowie die drauf befindlichen Apps mit sicheren Passwörtern und einer 2-Faktor-Authentifizierung gesichert sein.

2) Das Zuhause schützen
Sollten daheim smarte Komponenten oder gar ein Smart Home eingerichtet sein, ist es sinnvoll, diese abzuschalten oder in den Abwesenheitsmodus zu versetzen. Wenn zudem das Heim-WLAN ausgeschaltet ist, haben Cyberkriminelle keine Chance während der Abwesenheit das heimische Netzwerk zu infiltrieren.

3) Internet im Urlaub?
Selbstverständlich, denn wer will nicht auf dem Laufenden bleiben, seine sozialen Kontakte pflegen oder andere an der eigenen Reise teilhaben lassen. Allerdings sollte man darauf achten, ausschließlich auf sicheren Seiten zu surfen (erkennbar an https://) und alle anderen Web-Destinationen zu vermeiden. Wer es besonders sicher mag, der kann sich einen geschützten VPN-Tunnel für jeglichen Internetverkehr einrichten.

4) Online-Shopping und -Banking tunlichst vermeiden
Endlich hat man Zeit, in den Weiten des Internet-Shopping-Universums zu stöbern. Auch hier ist darauf zu achten, dass der Shop sicher ist und die Internet-Adresse mit einem https://

beginnt. Niemals sollten Bestellungen über Links zu Bank- oder anderen Geschäftsseiten aus E-Mails heraus für Käufe genutzt werden. Und unter keinen Umständen sollten Bankdaten angegeben werden, sollte es sich nicht um eine sichere Bezahloption eines bekannten Online-Anbieters handeln. Übrigens: es ist ratsam, das Limit für Bezahlungen bei der Bank auf einen möglichst niedrigen Wert zu setzen.

5) Der Klassiker: die unerwartete Geschäfts-E-Mail
Kommt trotz der Abwesenheit eine unerwartete und seltsame Nachricht von einem Mitarbeiter oder Geschäftspartner, sollte man nicht direkt darauf antworten und schon garnicht auf einen zugesendeten Link klicken. Denn die Chance einer zielgerichteten Phishing-E-Mail ist groß. Besser ist es, die Nachricht erst einmal per Telefon, SMS oder Firmen-Chatprogramm zu verifizieren.

Wer diese fünf Tipps beachtet und im Urlaub wachsam bei jeglicher Kommunikation im Internet ist, hat beste Chancen, die Ferien ohne Cyberfrust zu genießen. Egal wo man seine freie Zeit genießt, gilt: Finger weg von dubiosen Seiten, Angeboten oder Nachrichten.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de