Süße Kleinigkeit? Von wegen: das Easter Egg von heute hat es faustdick hinter den Löffeln

3 Tipps von Sophos fürs sichere Verschenken von digitalen Ostereiern

Wiesbaden, 11. April 2017. Völlig überraschend steht Ostern vor der Tür. Und so werden am Wochenende für den Nachwuchs wieder fleißig „Ostereier" versteckt. Dabei ist das Osterei aus historischer Sicht keine Kleinigkeit, denn seine Geschichte geht auf die berühmten und kunstvollen Farbergé Eier zurück, die im russischen Zarenhaus als Verpackung für „Kleinigkeiten" wie teuren Schmuck dienten. Einen weiteren historischen Eindruck hinterließen Ostereier, genannt Easter Eggs, in der Software-Industrie. Programmierer versteckten kleine Programme und Botschaften in ihrer Software, die nur durch nicht-offizielle Tastenkombinationen gestartet werden konnten. Eines der bekanntesten Easter Eggs ist wohl der Flugsimulator, der sich in Microsoft Excel 97 versteckte.

Nun geht es also wieder um Überraschungen für die Kleineren, und während man früher Kinderaugen noch mit ein paar Süßigkeiten und Kuschelhasen zum Leuchten bringen konnte, müssen heute andere Geschütze sein: Von Spielwaren und Unterhaltungselektronik, über Computer und Zubehör bis zu Smartphones, Tablets und Wearables hat der Osterhase alles dabei. Und weil Elektronik heute erst richtig Spaß macht, wenn sie mit dem Internet agiert, werden vermutlich viele kleine internetfähige Gadgets (Internet of Things) im Nest liegen. Dass damit aber auch Gefahren für Privatsphäre und persönliche Daten verbunden sind, werden am Ostersonntag wenn all diese Geräte möglichst schnell online gebracht werden, nur wenige beachten.

Bevor man jedes neue Gerät gleich hopplahopp online stellt, sollten ein paar Sicherheitsaspekte bedacht werden:

1.Vor dem Kauf informieren: Ist das ein sicheres Gerät?
Vor der Anschaffung des Gadgets sollte man sich informieren: Wurde das Gerät bereits getestet? Fachzeitschriften geben oft einen hilfreichen Überblick. Auch Verkäufer können gute Praxis-Tipps geben. Und last but noch least: eine schnelle Google-Suche, ob das gewünschte Gerät vielleicht schon einmal gehackt wurde, ist auch nicht verkehrt.

2. Gastnetzwerk für IoT-Geräte einrichten
Fast jeder WiFi-Router verfügt heute über die Möglichkeit, ein Gastnetzwerk einzurichten. Nutzen Sie das aus. So verhindern Sie, dass das neue IoT-Gadget Zugang zu Ihrem regulären Netzwerk bekommt.

3. Verwenden Sie die aktuellsten Software-Versionen
Sollte eh klar sein. Aber beim Einbinden neuer Geräte ins Netzwerk gilt es um so mehr: Nutzen Sie die aktuellsten Versionen für sämtliche Geräte, die mit dem Internet verbunden sind, wie PC, Laptop, TV. Und spielen Sie die Sicherheitspatches der Hersteller ein, sobald diese verfügbar sind. Die haben meistens ihren Sinn.

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. Weitere Informationen unter www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
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 +172 4536839
sophos@tc-communications.de