



Einfach und schnell: PCR-Testgerät für daheim Neuer SMS-Betrug aus Großbritannien bald auch bei uns?

Pandemien und andere Krisensituationen rufen zumeist auch Cyberkriminelle auf den Plan. Ein aktuelles Beispiel aus Großbritannien beweist kriminelle Kreativität, die bald auch anderswo Nachahmer finden könnte: gefälschte Kurzmitteilungen bieten via Link ein PCR-Testgerät für Zuhause an.

Sophos beschreibt den britischen Betrugsversuch und gibt Tipps für mehr Achtsamkeit beim SMS-Öffnen.

Das Redaktionsteam des Sophos Blogs [Naked Security](#) wurde von einem Leser über diesen aktuellen SMS-Betrug informiert: er hatte vermeintlich eine Kurzmitteilung vom nationalen Gesundheitsdienst NHS (National Health Service) erhalten, der die Impfungen gegen das Coronavirus verwaltet und landesweit freie Testmöglichkeiten anbietet. Die gefälschte SMS versprach via Link ein PCR-Testgerät für zuhause. Ein scheinbar attraktives Angebot und klug eingefädelter Fake, denn zunächst einmal sind Textnachrichten von Behörden in Großbritannien nichts ungewöhnliches, nutzt die dortige Regierung diese doch tatsächlich für unterschiedliche Zwecke, zum Beispiel 2FA, Erinnerungen oder Benachrichtigungen.

PCR-Heimtest-Gerät als toller Service

PCR-Tests sind genauer in der Erfassung einer Infektion und stehen u.a. für im Schnelltest positiv Getestete kostenfrei zur Verfügung – in Großbritannien wie in Deutschland. Aber anders als in Deutschland erhält man im Königreich per Post einen einmaliges Test-Set, das man dann an das Labor sendet. Dieses Verfahren dauert natürlich länger und verlängert auch die verpflichtende Quarantäne bei Symptomlosigkeit. Für viele (besonders Selbständige), deren Beruf nicht einfach im Home-Office ausgeführt werden kann, wie Handwerker, Berater oder mobile Pflegekräfte, käme da ein PCR-Testgerät für Zuhause gerade richtig. So könnten sie täglich ihre Termine sogar mit einem frischen und verifizierbaren COVID-Testergebnis wahrnehmen.

Ein dem Anschein nach also zunächst einmal sinnvolles (Fake-)Angebot und somit für die Cybergangster allemal den Betrugsversuch wert. Ob so ein Gerät für die Konsument:innen überhaupt bezahlbar wäre und ob die Ergebnisse sich dann verlässlich und sicher online bestätigen ließen, steht auf einem anderen Blatt. Aber in einer Welt, in der Produkte innerhalb von Stunden mit sicherer Bezahlung an die Haustür geliefert werden, Mobiltelefone mit ihren hochauflösenden Kameras jeden Flecken der Erde in Echtzeit streamen und Bürger eine Spritztour ins Weltall machen können, scheint auch ein Hausgerät für PCR-Tests keine Absurdität.

Wie also mit scheinbar „offiziellen“ SMS oder E-Mail verfahren?

Es kommt eine sehr echt anmutende SMS – oder auch E-Mail – vom örtlichen Gesundheitsamt, von der Bezirksverwaltung, oder direkt vom Gesundheitsminister? Ein kleiner Check reicht oftmals aus, um gefälschte Links zu entlarven:

- Ist diese Nachricht wirklich wahrscheinlich? Z.B. mit einem Angebot für ein PCR-Testgerät für zuhause? Sehen der Link und die URL tatsächlich echt und vertrauenswürdig aus?
- „Offizielles“, gültiges Testergebnis von zuhause aus? Ohne Labore oder andere Auswertungsstellen, die Ergebnisse an das RKI (Robert Koch Institut) übermitteln? Unwahrscheinlich.



- Und schließlich: würde man über solch eine neue Errungenschaft tatsächlich nur über SMS (oder E-Mail) informiert? Ohne dass in den Medien zuvor darüber berichtet worden wäre? Eher nicht.

Die Sophos-Expert:innen haben sich den Link in der britischen SMS genauer angesehen, aber bislang funktioniert die Webseite, auf die er leitet, nicht korrekt. Alles, was sie dem Webserver entlocken konnten, war eine kurze Liste von Dateinamen und eine Seite mit der Meldung Error 600. Nur existieren HTTP-Codes über 599 gar nicht...

Trotzdem ist das Beispiel, das so oder so ähnlich sicherlich auch in anderen Regionen Nachahmer finden kann, eine weitere wichtige Erinnerung daran, wie perfide die Cybergangster ihre Netze mittlerweile auswerfen und aktuelle Themen für ihre kriminellen Zwecke nutzen.

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/>

Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

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