Vorsicht vor Betrügern im Internet – Was beim Kauf von Corona-Schnelltests im Netz zu beachten ist

Zur Eindämmung der Corona-Pandemie setzt die Bundesregierung zusätzlich auf vermehrtes Testen. Durch kostenlose Schnelltests in Testzentren, Arztpraxen oder Apotheken sowie Selbsttests für die Eigenanwendung zu Hause sollen Infizierte schnell identifiziert werden. Die ersten drei Anbieter für Corona-Schnelltests zur Eigenanwendung durch Laien wurden diese Woche vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) zugelassen.

3 – 2 – 1 – Meins! Doch warum bekomme ich das gewünschte Produkt nicht geliefert? „Fake Shops locken Kunden meist mit besonders günstigen Angeboten zu einem Produkt, bei dem die Nachfrage aktuell sehr hoch ist oder die Verfügbarkeit sehr gering“, erklärt Dr. Peter Mayer von der Forschungsgruppe SECUSO am Karlsruher Institut für Technologie. „Probleme mit solchen betrügerischen Online-Shops verschärften sich in der ersten Zeit der Pandemie, da zum Beispiel Desinfektionsmittel und medizinische Schutzausrüstungen rar waren und die Bürgerinnen und Bürger aufgrund des Lockdowns vermehrt im Internet bestellt haben. Wir vermuten daher, dass mit der Zulassung von Schnelltests für die Eigenanwendung ein ähnlicher Trend festzustellen ist“, ergänzt Anne Hennig, die als Wissenschaftliche Mitarbeiterin in der Forschungsgruppe das Projekt INSPECTION unterstützt.

In dem vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekt forschen Dr. Peter Mayer und Anne Hennig (M.A.) gemeinsam mit den Partnern der MindUp Web + Intelligence GmbH, der BDO AG Wirtschaftsprüfungsgesellschaft und weiteren assoziierten Partnern zum Thema Fake Shops im Internet. Eine Vorgehensweise von Betrüger ist es, Sicherheitslücken in bestehenden Webseiten von Unternehmen, Vereinen oder Privatpersonen zu nutzen. Die Hacker verschaffen sich Zugang zur Web-Plattform der Betroffenen und hinterlassen im Quellcode der Webseite eine Weiterleitung zu ihrem Fake Shop. Die Geschädigten bekommen davon oftmals gar nichts mit, da die Betrüger lediglich den Namen und damit die Sichtbarkeit der Webseite in den Rankings der Suchmaschinenanbieter nutzen. Ziel des Projekts INSPECTION ist es, gehackte Webseiten ausfindig zu machen, das Vorgehen der Betrüger im Internet nachvollziehen zu können und einen geeigneten Kommunikationsweg zu entwickeln, um betroffene Webseitenbetreiber:innen zu informieren.

„Wichtig ist es, dass Sicherheitslücken schnell geschlossen werden, um Schaden zu vermeiden. Dabei trifft es nicht nur den Endverbraucher, der um sein Produkt betrogen wurde, sondern auch das Unternehmen, dessen Image durch den Betrug geschädigt worden ist“, erläutert Dr. Peter Mayer. Webseitenbetreiber:innen sollten dabei darauf achten, dass die Webseiten-Plattform regelmäßig aktualisiert wird. Wird ein Content-Management-System (CMS) wie Wordpress, Joomla oder Typo3 genutzt, sollten nicht nur die Plattformen an sich, sondern auch die Erweiterungen, sogenannte Plugins, auf dem aktuellsten Stand sein. „Aber auch unsichere Passwörter für den Login auf die Webseiten-Plattform sind ein Einfallstor für Betrüger“, erklärt Anne Hennig.

Und wie können Kund:innen sich vor Fake Shops schützen? „Das wichtigste ist, zunächst eine Plausibilitätsprüfung durchzuführen“, rät Prof. Melanie Volkamer, Leiterin der SECUSO Forschungsgruppe, „Wie wahrscheinlich ist es, dass der Malermeister aus Norddeutschland mir Corona-Schnelltests verkauft? Erscheint es denn logisch, dass bei diesem Anbieter Schnelltests nur halb so teuer sind, als bei allen anderen? Diese Fragen sollte ich mir zuerst stellen.“ Ein Set mit 20 bis 25 Testkassetten für den medizinischen Gebrauch kostet aktuell zwischen 120 und 200€. Wie teuer Schnelltests für den Laiengebrauch sein werden ist noch nicht bekannt.

Gütesiegel, wie das Trusted-Shop-Label oder das S@fer Shopping Siegel des TÜV Süd, können ein weiteres Indiz dafür sein, dass der Shop vertrauenswürdig ist. „Aber auch hier ist Vorsicht geboten“, meint Volkamer. Betrüger könnten die Siegel einfach kopieren oder eigene Siegel erfinden, um Seriosität vorzutäuschen. Hinter vertrauenswürdigen und aktuell gültigen Gütesiegeln steht ein Zertifikat, das der Siegelanbietende ausgestellt hat. Mehr Informationen zu Gütesiegeln für den Online-Handel gibt die Initiative D21 (Link: https://initiatived21.de/artikel-guetesiegel-beim-online-kauf/).

„Misstrauisch sollte man werden, wenn der Shop als Zahlungsmittel ausschließlich Vorauskasse oder Zahlung per Kreditkarte anbietet“, so die IT-Sicherheitsexpertin. Insbesondere wer per Vorauskasse bezahlt und die Ware anschließend nicht erhält, hat kaum Chancen, sein Geld wiederzubekommen. Ist auf der Shop-Seite zudem kein Impressum angegeben oder sind die angegebenen Kontaktdaten nicht erreichbar, sollte man Abstand von diesem Anbieter nehmen, meint Volkamer. „Ist man dennoch unsicher, hilft eine Websuche. Oftmals warnen zum Beispiel Verbraucherzentralen oder Sicherheitsbehörden vor betrügerischen Shops.“

Doch auch wenn ein Webshop vertrauenswürdig erscheint – solange er keine vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) zugelassenes Produkt für die Eigenanwendung durch Laien anbietet, sollte man dort nicht bestellen. Das BfArM hat aktuell drei Anbieter zugelassen. Die Liste wird durch das Institut kontinuierlich aktualisiert.

„Grundsätzlich raten wir immer dazu, nicht überstürzt zu handeln. ‚Slow down‘ ist das grundsätzliche Gebot bei Fragen der IT Sicherheit - nicht nur beim Online-Shopping,“ meint die Leiterin der SECUSO Forschungsgruppe.

Weiterführende Informationen
Forschungsgruppe SECUSO: https://secuso.aifb.kit.edu/
Projekt Inspection: https://web-inspection.de/
Liste zugelassene Tests des BfArM zur Eigenanwendung durch Laien: https://www.bfarm.de/DE/Medizinprodukte/Antigentests/_node.html
Inititative D21 – Gütesiegel beim Online-Kauf: https://initiatived21.de/artikel-guetesiegel-beim-online-kauf/

Kontaktdaten
Prof. Melanie Volkamer: melanie.volkamer@kit.edu
Dr. Peter Mayer: peter.mayer@kit.edu