Weihnachtspaketbetrug

Bitte beachten Sie unsere Warnung zum Weihnachtspaketbetrug. Er fällt dieses Jahr besonders intensiv aus, weil wohl nie zuvor so viel an Weihnachten über das Internet bestellt wurde wie in 2022:

DHL-Mail-Betrug ähnlich wie in Vorjahren

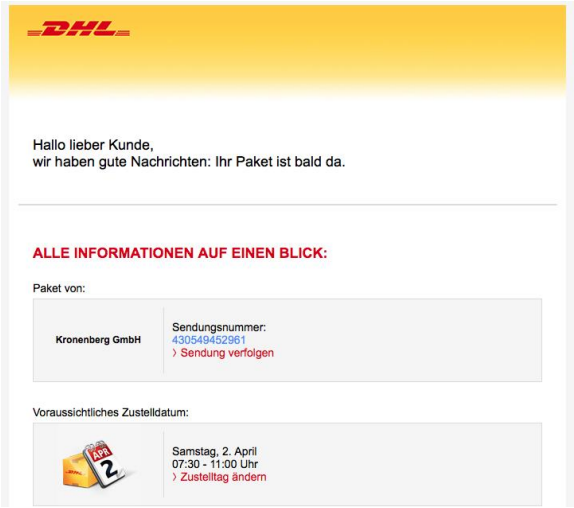
Der Betrug, der als Deckmantel den weit verbreiteten Paketlieferanten **DHL** verwendet, funktioniert nahezu identisch wie den letzten Jahren auch. Die Betrugsmasche wurde kaum geändert, trotzdem findet sie regelmäßig tausende Opfer. Bitte lesen Sie unseren immer noch aktuellen Newsletter aus einem Vorjahr, um sich zu informieren:

Dieses Weihnachtspaket bringt Ärger

Jedes Jahr an Weihnachten werden so viele Pakete wie sonst kaum im Laufe eines Jahres versendet. Das wissen auch die Online-Betrüger und reaktivieren gerne an und kurz vor den Feiertagen die zwar bekannte, aber trotzdem immer wieder funktionierende Masche der gefälschten Paketdienst-Zustellungsmails. Oft ist von nicht zustellbaren Paketen die Rede, mehr Informationen soll es dann im Anhang geben oder nach Klick auf einen Link in der Mail. Man wird neugierig und vermutet oder erhofft ein Weihnachtsgeschenk. Aber ein solcher Anhang enthält in Wirklichkeit Viren und Trojaner, der Link führt auf unseriöse Internetseiten.

Die echten E-Mails der Paketzulieferer enthalten zwar keine persönliche Ansprache und ebenfalls einen Link zum Anklicken (für die Sendungsverfolgung), aber die enthaltenen Daten dienen lediglich zur Information. Und die E-Mail enthält keinen Anhang. Betrügerische Mails behaupten hingegen meist, das Paket könne nur dann zugestellt werden, wenn ein Link angeklickt oder ein Anhang heruntergeladen wird.

Die echten E-Mails der Paketzulieferer sehen zum Beispiel so aus: →



Paket-Betrug auch per SMS

In besonderen Fällen gehen die Betrüger noch einen Schritt weiter und versuchen, per SMS Opfer zu finden. Eine SMS wird oftmals als persönlicher empfunden und die Menschen sind weniger vorsichtig, wenn sie den Inhalt lesen und darauf reagieren. Zwar ist der Betrug per SMS seltener, aber aufgrund der eben geschilderten Unvorsichtigkeit häufiger erfolgreich. Bitte lesen Sie unseren Newsletter aus der Vergangenheit, um sich zu schützen:

Gefährliche Paket-SMS im Umlauf

Zurzeit sind verschiedene betrügerische SMS im Umlauf, in den meisten Fällen geht es dabei um angebliche Paketzustellungen. Die Kriminellen machen es sich zu Nutze, dass wegen der Pandemie aktuell besonders viele Menschen im Internet einkaufen und entsprechend so viele Pakete ausgeliefert werden, wie nie zuvor. Sie versenden gefälschte Paket-SMS, in denen beispielsweise eine Lieferung angekündigt wird. Die SMS erhalten einen Link für angebliche weitere Informationen oder zur Sendungsverfolgung. Das klingt seriös und von dieser “Sendungsverfolgung” haben viele Nutzer auch schon mal etwas gehört. Tippt man den Link an, so wird allerdings eine Schadsoftware auf dem Handy installiert und keine Sendungsverfolgung geöffnet. Dieses Schadprogramm kann das Handy ausspähen, Kontakte auslesen und sogar das Handy kapern und weitere solche SMS an die Kontakte aus Ihrem Adressbuch versenden. Das kann Kosten verursachen! So verbreitet sich die betrügerische SMS nach dem Schneeballsystem immer weiter. Warnen Sie also auch alle Bekannten!

Wie erkenne ich die gefährliche SMS?

Von der betrügerischen SMS sind zahlreiche verschiedene Varianten im Umlauf, auch die Absendernummer ändert sich ständig. Die SMS ist aber fast immer so aufgebaut, dass erst ein kurzer Text auf ein Paket verweist und danach erscheint ein Link zum Antippen. Besonders “erfolgreich” sind die SMS, bei denen angeblich ein besonderer Umstand das Paket in der Auslieferung verhindert und der Nutzer so eher reagiert, also auf den Link tippt. Hier drei Beispiele, die wir selbst erhalten haben:

In anderen Varianten der SMS heißt es zum Beispiel:
– “Ihr Paket ist da. Letzte Chance es abzuholen …”
– “Ihr Paket wurde verschickt …”
– “Ihr Paket konnte nicht zugestellt werden …”
– “Ihr Paket kommt an, verfolgen Sie es hier …” oder
– “Dein Paket ist in der Warteschlange. Versand bestätigen …”

Was ist zu tun, wenn man die SMS erhält?

Der reine Empfang der SMS für sich gesehen ist (genau wie bei Spam-Mails auch) noch nicht gefährlich. Bedenklich wird es erst, wenn Sie den Link in der SMS auf einem Smartphone antippen. Dann wird nämlich im Hintergrund ein Schadprogramm installiert, das unter anderem die Kontakte auslesen und weitere SMS an die Nummern aus Ihrem Telefonbuch versenden kann. Wenn Sie die SMS erhalten, löschen Sie diese, ohne in der Nachricht etwas anzutippen. Wenn Sie den Link versehentlich doch angetippt haben, schalten Sie das Handy sofort in den Flugmodus. So können keine weiteren Nachrichten über Ihr Handy versendet werden. Die WLAN-Verbindung kann nun separat aktiviert werden, um eine Virenscanner-App aus dem Play Store

herunterzuladen. Zudem sollten Sie die installierten Apps kontrollieren und die zuletzt installierten Anwendungen löschen.
Das BSI (Bundesamt für Sicherheit in der Informationstechnik) rät außerdem dazu, den Mobilfunkanbieter zu informieren. Sollten tatsächlich SMS über Ihr Handy verschickt worden sein, so kann der Mobilfunkanbieter eventuell die Kosten erstatten oder weitere Kosten verhindern. Hierbei hilft auch die sogenannte Drittanbietersperre. Sie wird ebenfalls beim Mobilfunkanbieter eingerichtet und verhindert, dass Dritte über Ihre Handyrechnung Geld abbuchen können. Dieses Vorgehen wurde eigentlich als einfache Möglichkeit zum Bezahlen mit dem Smartphone entwickelt, kann aber auch von den Betrügern genutzt werden um an Ihr Geld zu kommen.

Die Gefahr besteht vor allem auf Android-Smartphones. Auf dem iPhone von Apple kann die Schadsoftware nicht so leicht installiert werden. Dennoch sollten Sie auch hier den Link nicht antippen. Bitte auch keinesfalls auf die SMS antworten oder sie anrufen. Bei Android-Smartphones kann man in den Einstellungen außerdem festlegen, dass Apps aus unbekannten Quellen nicht installiert werden dürfen. Auch ist es möglich, die Absendernummer zu blockieren, wenn Sie die SMS schon erhalten haben, um nicht noch weitere derartige SMS zu erhalten. Allerdings wechseln die Betrüger ständig die Nummern, sodass dies vermutlich nicht 100% davor schützen wird, die SMS noch einmal zu erhalten.

Woher haben die Betrüger “meine” Nummer?
Hierfür gibt es mehrere Möglichkeiten. Viele der angeschriebenen Nummern stammen offenbar aus einem Datenleck, das heißt, Ihre Kontaktdaten wurden bei anderen Unternehmen gestohlen. So wurden bspw. kürzlich durch ein Datenleck bei Facebook die Handynummern von einer halben Milliarde Menschen öffentlich, über sechs Millionen Deutsche sind davon betroffen. Auch bei der Telekom sind in den letzten Jahren immer wieder Millionen Kundennummern von Kriminellen gestohlen worden. Die Quellen, aus denen die Kriminellen Ihre Nummer haben könnten, sind also vielfältig. Die reine Tatsache, dass jemand Ihre Nummer hat, bedeutet also noch nicht, dass Sie einen Fehler gemacht hätten oder sich sofort Sorgen machen müssen. Erst das aktive Anklicken des Links in einer solchen SMS bringt Probleme. Fällt jemand auf die SMS herein und klickt den Link an, so können die Betrüger sogar auf die Kontakte dieser Person Zugriff nehmen. So verbreitet sich die SMS immer weiter. Natürlich kann es auch sein, dass die Kriminellen schlichtweg nach dem Zufallsprinzip millionenfach Handynummern anschreiben.
Quelle: Verbraucherzentrale.

Wie kann ich mich schützen?
Sie können nicht verhindern, dass Sie die betrügerische SMS erhalten. Auch wir haben die SMS schon mehrfach zugeschickt bekommen. Der einzige wirksame Schutz ist daher Aufmerksamkeit. Wenn Sie eine solche SMS erhalten, schauen Sie sich die SMS sehr gut an. Lesen Sie den Inhalt ruhig, langsam und mehrfach. In den meisten Fällen ist der Betrug dann recht einfach zu erkennen, denn die Links in den SMS führen zu kryptischen Seiten. In unserem Beispiel lautet die Adresse https://hairat32.co.uk/pkge/…. So sieht keine Internetseite von DHL, DPD oder UPS aus, der Betrug ist also sehr schnell zu erkennen. Doch manchmal geben sich die Betrüger auch mehr Mühe und verändern den Link so, dass er tatsächlich echt aussieht. Fragen Sie sich in so einem Fall immer: Erwarte ich derzeit überhaupt ein Paket? Falls ja, woher sollte der Paketdienst meine Handynummer haben? Ist der Inhalt der SMS plausibel? Tippen Sie im Zweifelsfall nie Links in SMS an, wenn Sie sich unsicher sind. Löschen Sie die SMS stattdessen direkt.
Quelle: BSI.

Quelle: https://levato.de/weihnachtspaketbetrug/