40. Info-Brief für @sse

Liebe Sicherheitspartnerinnen und Sicherheitspartner,

leider muss unser Aktionsbündnis aufgrund der andauernden Pandemie weiterhin ruhen. Wir möchten auch lieber HEUTE als MORGEN wieder mit Ihnen in Kontakt treten, Sie zur nächsten Supervision einladen, Infostände mit Ihnen durchführen und andere Senioren persönlich beraten. Sobald das wieder möglich ist, werden Sie von uns lesen.

Gerade im Moment sind die Ganoven kreativer denn je. Von der Betrugswelle mit gefälschten DHL-Nachrichten haben Sie bestimmt schon gehört oder gelesen. Sie nimmt kein Ende, so dass wir Sie intensiv darauf aufmerksam machen möchten.

Mit dieser neuen Masche missbrauchen Kriminelle die Marke DHL und versenden im Namen des Paketdienstleisters gefälschte E-Mails. Darüber sollen die Computer und Handys der Nutzer mit Schadsoftware infiziert werden.

POLIZEI
Nordrhein-Westfalen
Kreis Mettmann

Der Trick: Es soll der angebliche Zustelltermin verschoben werden.

Ein Paket ist auf dem Weg zu Ihnen. Im Zeitalter von Corona und dem extrem wachsenden Markt des Onlineshoppings ist das nichts Besonderes. Und genau darauf setzen die Kriminellen, die mit einer gefälschten E-Mail von DHL ankündigen, dass ein Paket unterwegs ist.

Wie bei DHL üblich, können sie praktischerweise über einen Link die Sendung verfolgen und nachsehen, wann das Paket bei Ihnen ankommt. Allerdings stammt die E-Mail nicht von DHL und steht mit dem Paketdienstleister auch in keinem Zusammenhang. Auch ein Paket für Sie ist nicht unterwegs.

Vielmehr versuchen Kriminelle, Ihren Computer mit einem trojanischen Pferd zu infizieren. Die Betrüger ändern permanent ihre Strategie und die betrügerischen E-Mails. Zuerst verzichteten sie auf einen Anhang, jetzt versenden sie nur noch eine Anlage.

Mit der Fälschung von E-Mails des Logistikkonzerns DHL haben sich die Betrüger bereits ein sehr großes Unternehmen ausgesucht. Die millionenfach versendeten Fälschungen mit DHL als

Absender kommen immer wieder zur richtigen Zeit am richtigen Ort an. Nämlich da, wo ahnungslose Kunden sehnlichst auf ein Paket warten und den Link zur Sendungsverfolgung bedenkenlos anklicken. Um die Trefferquote noch zu erhöhen verwenden die kriminellen jetzt weitere Markennamen.

So wird ein Paket von Amazon oder IKEA angekündigt. Die dazu passenden Logos sind ebenfalls in der E-Mail enthalten. Das schafft Vertrauen und sorgt dafür, dass noch mehr Opfer die Links anklicken und so zur weiteren Verbreitung des Spams beitragen.

Seit einiger Zeit kommen die gefälschten DHL-Mails im neuen Gewand in die Postfächer der Nutzer. Die Nachrichten der neuen Spam-Welle enthalten keinerlei Text mehr. Vielmehr befindet sich im Anhang eine scheinbar harmlose PDF-Datei. Diese enthält die eigentliche Paketankündigung und einen Link zur Sendungsverfolgung. Die PDF-Datei selbst enthält bisher keinen Virus. Erst bei einem Klick auf den Link zur Sendungsverfolgung wird der Trojaner auf den Computer oder das Smartphone heruntergeladen. Allerdings ist es denkbar, dass sich das ändert und zukünftig infizierte Anhänge versendet werden.

Der Versand der PDF-Datei ist ein geschickter Schachzug der Kriminellen. Dadurch erhöhen sich die Klicks, da Nutzer die E-Mail nicht mehr als Spam erkennen. Auch viele E-Mail-Programme sortieren die E-Mail nicht mehr als Spam aus.

Deswegen rät die Polizei:

- Bitte keine Links in PDF-Dateien von DHL anklicken! DHL versendet keine E-Mails mit PDF-Dateien!
- Am besten ist es, wenn diese gar nicht erst geöffnet werden!

POLIZEI
Nordrhein-Westfalen
Kreis Mettmann

Impressum / Kontakt
Herausgeber: Kreispolizeibehörde Mettmann
VUP/O, KP/O
Adalbert-Bach-Platz 1
40822 Mettmann

Ansprechpartner: Verkehrsunfallprävention:
02104/982-5110
Kriminalprävention:
02104/982-7700

E- Mail: info@seniorensicherheit-kreis-mettmann.de
Internetpräsenz: seniorensicherheit-kreis-mettmann.de