wahlkreisbuero@ulf-thiele.de

Betreff: Cyberkriminelle nutzen Corona für die Verbreitung von Schadsoftware aus

Von: "Informationssicherheit (LT)" <Informationssicherheit@lt.niedersachsen.de>
Datum: 18. März 2020 um 14:43:14 MEZ
Betreff: Cyberkriminelle nutzen Corona für die Verbreitung von Schadsoftware aus

Sehr geehrte Damen und Herren,
liebe Kolleginnen und Kollegen,

sicher haben Sie schon aus dem Medien erfahren, dass Cyberkriminelle das Thema Corona für Ihre Zwecke ausnutzen und versuchen, unter dem Schlagwort "Covid-19" oder „Corona-Virus“ per E-Mail oder durch manipulierte Webseiten Schadprogramme zu verteilen. In den meisten Fällen verfolgen sie das Ziel, Daten wie Passwörter oder Kreditkartennummern abzugreifen.

Nutzen Sie daher bitte offizielle Informationsquellen, um sich über Covid-19 zu informieren! Verlässliche Informationen finden Sie u.a. beim Robert-Koch-Institut unter https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/nCoV.html und der Bundeszentrale für gesundheitliche Aufklärung https://www.infektionsschutz.de/coronavirus-sars-cov-2.html.

Seien Sie dagegen generell vorsichtig beim Öffnen von unbekannten Dateien sowie elektronischen Nachrichten und überprüfen Sie Absender und enthaltene Verlinkungen. Auch Falschmeldungen oder sogenannte Kettenbriefe, die über Messenger-Dienste verbreitet werden, sollte kein Glauben geschenkt werden. Leiten Sie diese Nachrichten daher bitte nicht weiter. Sollten Sie in einer Nachricht aufgefordert/gebeten werden, die Informationen mit anderen Personen zu teilen, ist das übrigens bereits ein deutliches Zeichen für einen unseriösen Kettenbrief.

Beispiele für aktuelle Angriffe:
Sicherheitsforscher haben eine Angriffsvariante ausfindig gemacht in der eine offiziell anmutende Karte die vermeintliche Ausbreitung des Corona-Virus darstellen soll, doch darin ist ein Schadprogramm versteckt. Dieses liest sensible Daten aus, die im Browser gespeichert sind und leitet diese an die Angreifer weiter.

Außerdem warnte die Verbraucherzentrale NRW vor gefälschten E-Mails der Sparkasse, worin Kundinnen und Kunden über die angebliche Schließung einiger Filialen informiert und zur Überprüfung ihrer persönlichen Daten aufgefordert werden (s. folgende Abbildung). Über die Links in der E-Mail gelangen Betroffene zu einer gefälschten Anmeldemaske. Dort eingegebene Zugangsdaten würden dann direkt an die Betrüger weitergeleitet werden.

Umgang mit dem COVID-19-Erreger

18. März 2020 um 07:27

Sparkasse

Sehr geehrte Kundinnen und Kunden,

Ihre Sicherheit und Gesundheit und auch die unserer Mitarbeiter liegt uns sehr am Herzen.

Vor diesem Hintergrund haben wir uns dafür entschieden, unsere kleineren Filialen bis auf weiteres zu schließen.

Sehr gerne stehen wir Ihnen telefonisch, per E-Mail und in unserem Online-Banking auch im Chat persönlich zur Verfügung. Die SB-Bereiche sind uneingeschränkt nutzbar.

Bitte nehmen Sie sich deshalb die 2 Minuten Zeit, um

– Ihre Adresse(n)

– Ihre Telefonnummer(n)

– und Ihre E-Mail-Adresse(n)

zu überprüfen und gegebenenfalls zu aktualisieren, um weiterhin eine reibungslose Kommunikation bei anliegenden Fragen zu gewährleisten.

In diesen Tagen müssen wir es als Gemeinschaft dem Erreger so schwer wie möglich machen, sich schnell zu verbreiten.

Prävention ist keine Hysterie, und Ignoranz ist auch kein Mut! Wir hoffen sehr auf Ihre Solidarität und Ihr Verständnis.

Vielen Dank!

Mit freundlichen Grüßen

Ihr Sparkassenverband.

Jetzt prüfen >

Quelle: *Verbraucherzentrale NRW*

Seien Sie daher bitte weiterhin wachsam und vorsichtig und bleiben Sie gesund!

Liebe Grüße
Sabrina Hagemann

Niedersächsischer Landtag
Landtagsverwaltung
Hannah-Arendt-Platz 1, 30159 Hannover

Telefon: 0511 3030-2240
E-Mail: sabrina.hagemann@lt.niedersachsen.de *
* nicht zugelassen für digital signierte Dokumente