Achtung! Schadprogramm!
Informationsblatt für Geschädigte von Angriffen auf das Onlinebanking

Eine Information Ihrer Polizei

Sie sind Geschädigter eines Angriffes auf das Onlinebanking geworden!
Ursache dafür ist mit hoher Wahrscheinlichkeit das Einschleusen von Schadsoftware auf Ihren PC. Diese haben die Cyberkriminellen durch folgende Maßnahmen auf Ihren PC gebracht:
Sie wurden durch die Zusendung einer Spammail dazu gebracht, den Anhang unbedacht anzuklicken, Sie haben beim Besuch einer infizierten Webseite den unbemerkten Download der Schadsoftware ausgelöst oder ein infizierter Datenträger wurde am Computer benutzt.
Das führt dazu, dass die Schadsoftware jetzt alle Ihre Eingaben von Passwörtern und Zugangsdaten heimlich mitprotokolliert und an die Cyberkriminellen übermittelt! Außerdem können die Cyberkriminellen Ihren PC unbemerkt fernsteuern!

Bevor Sie Ihren PC wieder für das Onlinebanking, Shopping im Netz, Nutzung der Sozialen Netzwerke usw. nutzen können, müssen Sie Ihren Computer dringend von Schadsoftware befreien!
Es besteht sonst die akute Gefahr, dass Ihre Änderungen von Zugangsdaten oder die Eingabe von neuen Logindaten erneut in die Hände von Cyberkriminellen geraten.

Nutzen Sie bitte nachfolgende Hinweise, damit Sie Ihren Computer von Schadsoftware befreien. In der Regel sind Computer mit den Betriebssystemen von Microsoft von dieser Schadsoftware betroffen. Sollten Sie über ein anderes Betriebssystem verfügen, so wenden Sie die Hinweise und Programme, soweit möglich, analog an:

1. Nutzen Sie ein aktuelles Antivirenprogramm und prüfen Sie mit einem vollständigen Virenscan den Computer. Denken Sie dabei auch an normalerweise angeschlossene externe Datenträger! Den ausführlichen Virenscan finden Sie in der Regel im Hauptmenü der Schutzsoftware und muss meist manuell ausgeführt werden. Je mehr Daten auf den Datenträgern vorhanden sind, umso länger kann die Untersuchung dauern. **Wir empfehlen die Nutzung kostenpflichtiger Antivirensoftware, da diese in der Regel einen umfassenderen Schutz bietet als kostenfreie Antivirenprogramme.** Viele Hersteller bieten diese kostenpflichtigen Programme auch als zeitlich beschränkte Testversionen kostenfrei zum Download an. Ein Update des Antivirenprogrammes ist vor der Nutzung zwingend notwendig, um aktuelle Viren zu erkennen.

2. Nach Beendigung des Scans, wird in der Regel ein Virenbericht erstellt. Ggf. müssen Sie diesen über das Menü der Schutzsoftware aufrufen. Bringen Sie diesen Report als Ausdruck zur späteren Anzeigeerstattung mit zur Polizei.

3. Wurde Ihr Programm fündig, so löscht das Antivirenprogramm die Schadsoftware in der Regel automatisch. Alternativ stellen einige Programme die gefundenen Dateien auch in Quarantäne.

4. Laden Sie auf www.botfrei.de zusätzlich den **EU-Cleaner** herunter. Sie finden den Cleaner sowie eine Gebrauchsanleitung unter dem Webseitenmenü „Säubern“. Führen Sie damit ebenfalls eine vollständige Systemprüfung (Haken setzen) aus.

5. Eine Garantie, dass die benutzten Antivirenprogramme Ihr System zu 100 % wieder säubern, kann nicht gewährt werden. Ziehen Sie eine vollständige Neuinstallation Ihres Systems in Betracht.
   Auf https://www.botfrei.de/neuinstallation.html finden Sie ebenfalls Informationen dazu. Bedenken Sie zuvor die Sicherung Ihrer persönlichen Dateien durch ein Backup - aber erst nach einem umfassenden Virenscan und Entfernung der Schadsoftware!

6. Bei einer alternativen Wiederherstellung aus einer vorherigen Sicherung kann nicht ausgeschlossen werden, dass auch hier schon die Schadsoftware enthalten ist. Diese Wiederherstellung kann jedoch genutzt werden, um noch wichtige persönliche Daten vor einer Neuinstallation oder Formatierung zu retten.

7. Nach der erfolgreichen Durchführung der Punkte 1 bis 4 oder der Neuinstallation Ihres Systems müssen Sie nun besonders in Ihren Mailaccounts (z.B. gmx, web.de, t-online usw.) überprüfen, ob dort fremde Kontakt- oder Weiterleitungsadressen hinterlegt sind. Hier besteht sonst die Gefahr, dass Cyberkriminelle nachfolgende Änderungen von Zugangsdaten (Punkt 8) mitbekommen. Melden Sie gefundene Auffälligkeiten ebenfalls der Polizei.
   Beachten Sie dabei, ob Sie die Mails direkt in dem Account bei Ihrem Mailanbieter aufrufen oder Programme wie Outlook oder Thunderbird zum Aufrufen und Lesen nutzen. In diesen Fällen werden die Mails und Datenanhänge auf ihren PC heruntergeladen.

8. Im Anschluss müssen Sie unbedingt die Zugangsdaten zu allen Ihren genutzten Diensten (z.B. Onlineshopping, Mail, Soziale Netzwerke, Onlinebanking usw.) ändern. Vor Ihrem Geldinstitut werden Sie in der Regel neue Zugangsdaten erhalten. Bei anderen Diensten ändern Sie die Passwörter gemäß der Empfehlungen, die Sie auf dem Ratgeber Internetkriminalität finden (http://www.polizei-praevention.de/themen-und-tipps/basisschutz-hard-software.html#c549).
   Eventuell haben die Cyberkriminellen bereits Ihre Zugangsdaten geändert, so dass Sie mit Ihrem bisherigen Passwort keinen Zugriff mehr erhalten oder die Passwortänderung nicht durchführen können.
   Nehmen Sie in einem solchen Fall sofort Kontakt zum Diensteanbieter auf und teilen Sie Ihre Erkenntnisse ebenfalls der Polizei mit!

9. Sollten Sie durch die Schadsoftware keinen Zugriff mehr auf Ihren Computer haben, so können Sie selbststartende Datenträger (CD, DVD oder USB-Stick) zur Rettung verwenden, die eine entsprechende Antivirensoftware beinhaltet. Informationen dazu finden Sie z.B. auch bei botfrei.de auf https://www.botfrei.de/rescuecd.html

Für weitere Fragen wenden Sie sich an Ihre zuständige Polizeidienststelle oder stellen Sie „Ihre persönliche Frage“ zu Cybercrime an den ‚Ratgeber Internetkriminalität’ auf www.polizei-praevention.de.

POLIZEI
NIEDERSACHSEN

Herausgeber:
Landeskriminalamt Niedersachsen, Zentralstelle Cybercrime und Zentralstelle Prävention , Am Waterlooplatz 11, 30169 Hannover

Stand: Januar 2015