EUROPEAN-NEWS-AGENCY.COM

EUROPEAN NEWS AGENCY

International Press Service

Ressort: Internet und Technik

Cybercrime aktuelle Warnung Insiderinfos 09.05.2026

Weltweit, 09.05.2026 [ENA]

Berichte, Warnungen, Präventionen gegen den sogenannten Cybercrime gibt es inzwischen Unzählige im Internet, bei Vorträgen, auf Messen, bei der Polizei. Und alle wissen, das in gewissen Bereichen die Zahlen nach oben schnellen. Viele Betroffene melden jedoch diese Probleme nicht.

Cybercrime, das beschreibt eigentlich erst einmal ein Phänomen, von dem man auf mehreren Wegen, meist unverschuldet, betroffen sein kann. Hacking, Phishing, Fake Emails, DDos – Attacken, Ransomware, Malware, Unverschuldet, das bedeutet, ein Firmenrechner wird von aussen gehackt und dann als Einfallstor ins Netzwerk der betreffenden Firma genutzt, um Schaden in Form von Verschlüsselungen, Löschungen oder Datenklau anzuwenden. Unverschuldet nenne ich aber auch, wenn ein Mitarbeiter aus Unkenntnis z.B. wegen fehlender Schulung eine vertrauenswürdige Email öffnet und dann einen Link benutzt, der Schadsoftware auf dem Rechner installiert. Dank KI werden sich im Cybercrime – Bereich die Möglichkeiten um ein Vielfaches erweitern.

Ich möchte aber hier und heute nicht auf den bekannten alten Kamellen rumreiten, sondern eine vielleicht auch nicht neue, aber besonders trickreiche Masche aufmerksam machen, die keiner, sei er auch noch so schlau, im Vorfeld entdecken kann. Und die geht so: Vorbei sind ja längst die Zeiten, wenn sie Spiele oder Anwendungssoftware kaufen, das ihnen nach Tagen eine Pappverpackung, womöglich mit Handbuch, einer DVD und einer Karte mit einer Lizenznummer zugeschickt wird; natürlich nicht: Alles wird online abgewickelt, im Regelfall bekommen sie einen Downloadlink, die Seriennummer mitgeteilt, zahlen per Paypal oder Kreditkarte.

Sie installieren das Spiel oder die Software, geben die Seriennummer ein, das Produkt wird freigeschaltet und läuft, fertig aus. Vielleicht prüfen sie später noch ob nicht zuviel abgebucht wurde aber wenn alles korrekt ist wunderbar. Nach einer Woche ist das Ganze vergessen und sie nutzen die Software. Das ist völlig normal heutzutage, Plattformen wie Steam oder Battle.net, um mal in Sachen 2 zu nennen, machen das ruckzuck möglich. Diese Plattformen gibt es auch für Anwendersoftware. Insbesondere werden dort Produkte, die viele Anwender nutzen, angeboten. Das betrifft Betriebssysteme, Office – Versionen und Sicherheitssoftware, um mal 3 Gruppen zu nennen.

Diese Großhändlerplattformen funktionieren wie Amazon, Kaufland oder Mediamarkt: Dort tummeln sich im Marketplace eigenständige Händler, die gar nichts mit den Plattformgeber zu tun haben, die Händler

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

zahlen im Zweifelsfall eine Abgabe oder Prozentanteil vom Umsatz, um die namenhaften Plattformen nutzen zu können und mehr Besucher zu bekommen. Man schließt also nicht mit den Plattformgeber, sondern dem Händler einen Vertrag. Da nicht nur die Plattformseiten, sondern auch die Händlerseiten in einwandfreiem Deutsch sind, scheut man auch keinen Kauf. Denn zusätzliche Sicherheiten sollen so einige Logos wie Trusted Shop usw. liefern, die aber nicht immer legitim verwendet werden.

Oftmals stellt sich erst hinterher, wenn überhaupt, heraus, wer letztlich der Händler ist und wo dieser seinen Sitz hat. Erst kürzlich habe ich bei mediamarkt.de ein Tablet und 3 USB Sticks gekauft, alle Preise sensationell günstig gegenüber den in Deutschland marktüblichen Preisen. Das Tablet kam dann aus Bulgarien, die Sticks aus Shenzhen China. Okay. Jetzt zurück zu meiner aktuellen Warnung, denn sie sind ja alle schon auf meine angekündigten Insiderinfos gespannt. Also ich habe auf der deutschen Großhändlerseite nach dem Programm Kasperksy Total Security gesucht und rasch ein paar Händler gefunden.

Natürlich sind die Angebote häufig günstiger als beim Originalhersteller, was nichts damit zu tun hat, das irgendetwas nicht in Ordnung ist. Es sei denn die Preisunterschiede sind extrem, Windows 11 als Betriebssystem für 3.95 Euro wäre schon verdächtig. Okay. Nachdem ich das Produkt ausgewählt hatte, mußte ich, wie üblich, auswählen, welchen Zeitraum und wieviel Geräte ich schützen möchte. Ich wählte wegen des Preises erst einmal 1 Gerät für 1 Jahr aus. Nach der Zahlung mit Kreditkarte bekam ich einen Downloadlink und eine Lizenznummer mitgeteilt. Alles funktionierte, ich habe mir dann bei Kaspersky Deutschland ein Konto erstellt und die Lizenznummer dort eingetragen. Ich bekam Updates usw. Alles lief normal.

Dann kam die Meldung von Kaspersky, das Produkt „ Total Security „ sei veraltet und auf die neue Version „ Kaspersky Premium „ upgegradet. Offensichtlich hatte die Premium Version aber mehr Programmteile, denn laufend kamen Meldungen, was ich doch nur noch zu aktivieren hätte, weil es in meinem Paket drin sei. Ich habe immer abgelehnt und irgendwann dann mein, vermeintlich MEIN Konto aufgerufen, und nanu, da sah ich plötzlich, mein Abo schütze 10 Geräte. Wieso das, ich hatte lt. Bestellung nur für 1 Gerät bestellt. Und nicht nur das: Abo stand da. Ich habe ja extra 1 Jahr ausgewählt wie ich eben kein Abo wollte. Aber angeblich kann man ja das Abo deaktivieren. Denkste.

Jetzt sehe ich auch, der vermeintliche Händler hat SEINE Email, die beim Konto mit 3 Sternen mittendrin dargestellt ist, bei dem Abschluß eingegeben. Und weil ich logischerweise seine Email nicht habe, konnte ich mich auch nicht in das Konto einloggen, auch Passwort – Vergessen – Anfragen würden ja nicht an mich gehen, sondern an seine Email. Mit meinen damals nach der Bestellung angelegten Daten konnte ich rein gar nix anfangen. Das bedeutete auch: Ich konnte das Abo nicht deaktivieren, und bei 10 aktivierten Geräten würde auf mich eine nicht unerhebliche Summe zukommen. Und ich wußte ja auch nicht auf

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

wieviel Jahre er das abgeschlossen hatte.

Jetzt ging das Drama los. Ich habe dann mit Kaspersky Deutschland Kontakt aufgenommen, ich nehme es vorweg. Hilfe = Null. Zuerst teilen die mir mit, mit meiner regulären Email wäre kein Abo abgeschlossen. Sie wollten die komplette Email des Händlers haben, woher sollte ich die aber bekommen ? Dann wollten sie den Aktivierungscode haben, auch den konnte ich nicht nennen weil ich keine Daten ohne Anmeldung abfragen konnte. Über die Lizenznummer wollten sie aber den Account nicht sperren. Also wie gesagt keine Hilfe, obwohl jetzt klar war, hier stimmt was nicht. Da ich keine Lust hatte, in Kürze, nämlich zum 30.5.2026, eine mir unbekannte Summe abgebucht zu bekommen, habe ich einen IT Spezialisten zu Rate gezogen.

Schlaue Leute werden jetzt vielleicht sagen, warum ich nicht bei der Bank die Abbuchung blockiert habe. Das geht im Vorfeld nicht, selbst wenn ich die Kreditkarte sperre, werden angemeldete Abbuchungen noch ausgeführt, diese müssen dann umständlich per Formular zurück gefordert werden und ich muß belegen, das das Abo gekündigt war. Und das ist es ja nicht, und wenn dann noch das Geld ins Ausland geht, ist es weg. So einfach ist das. Der IT Spezialist hat es dann geschafft, Zugriff auf das Konto zu erlangen: Erstmals konnte ich sehen, welche komplette Email der Händler hat. Ich konnte sehen, wer der Händler ist und wo der sitzt, und jetzt zeigt sich, das eine Geldrückholung faktisch unmöglich ist.

Die Firma hat ihren Sitz in Vietnam und die Gelder werden über den gleichen Firmennamen mit Sitz in Zypern abgewickelt. Interessanterweise hat er als Zahlungsmittel den Abos eine Mastercard eingetragen, die nicht meine ist. Wir haben das Zahlungsmittel angeklickt um es zu bearbeiten. Die nächste Verwunderung: Im „ Hintergrund „ war eine Art Verknüpfung mit meinen VISA Card Daten. Keine Ahnung, wie das geht und warum dieser Umweg. Ich habe mein Abo gestoppt, weil ich jetzt auch darauf Zugriff hatte. Besonders interessant fand ich den Einblick in das Rechnerimperium, das der Händler verwaltete.

Auf einer Internetseite des Kontos waren 193 Rechner aufgelistet, die alle Kaspersky Produkte bei dem Händler gekauft hatten. Ich konnte alle Rechnernamen, auch meinen, einsehen und auch sehen, wie lange die Abos, und alle hatten ein aktives Abo, was für ein Zufall, noch liefen. Interessant war auch, der Händler konnte nicht nur sehen, welche Rechner gerade online waren, er konnte bei jedem Rechner eine Kurz- oder Komplettanalyse starten, was immer das bedeutete. Mir hat das gereicht und der IT Spezialist hat das Konto verlassen, vorher die Verknüpfung zu meinem Rechner gelöscht.

Ich habe dann 3 Dinge unternommen: Die Kreditkarte zur Sicherheit trotzdem sperren lassen, Kaspersky Deutschland über den möglichen Betrug informiert, worauf sie nur geantwortet haben, das wäre ein Vertrag mit der vietnamesischen Kaspersky Firmierung, ich müßte mich dorthin wenden. Die Cybercrime

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Stabsstelle der Polizei Hannover bestätigte mir derweil, das ein Vorgehen gegen eine vietnamesische Firma fast unmöglich und extrem zeitaufwendig sei, die Frage wäre schon ob überhaupt eine Zusammenarbeit zwischen Deutschland und Vietnam wegen Datenaustausch stattfinden würde und wie lange es dann dauern würde, bis irgendwelche Maßnahmen eingeleitet würden. Von Anzeigen usw. hat man mir daher gleich abgeraten.

Insofern fand ich von einer anderen Polizeidienststelle die Anmerkung interessant, das es schon bei manchen EU Ländern mangelnde polizeiermittelnde Zusammenarbeit geben würde. Wurde da der Name Spanien genannt ? Ich weiß es nicht mehr. Natürlich mußte ich bei den Screenshots, die ich als Beweissicherung gemacht habe, bei der Veröffentlichung hier alle relevanten Daten, die auf Kunden oder die Firma schließen lassen, schwärzen. Denn ohne Ermittlung und Feststellung handelt es sich hier um einem Verdachtsfall, wenn auch vieles für mehr spricht.

Bericht online lesen:
https://romeoritter.en-a.de/internet_und_technik/cybercrime_aktuelle_warnung_insiderinfos_09052026-93634/

Redaktion und Verantwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV: Uwe Hildebrandt

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com