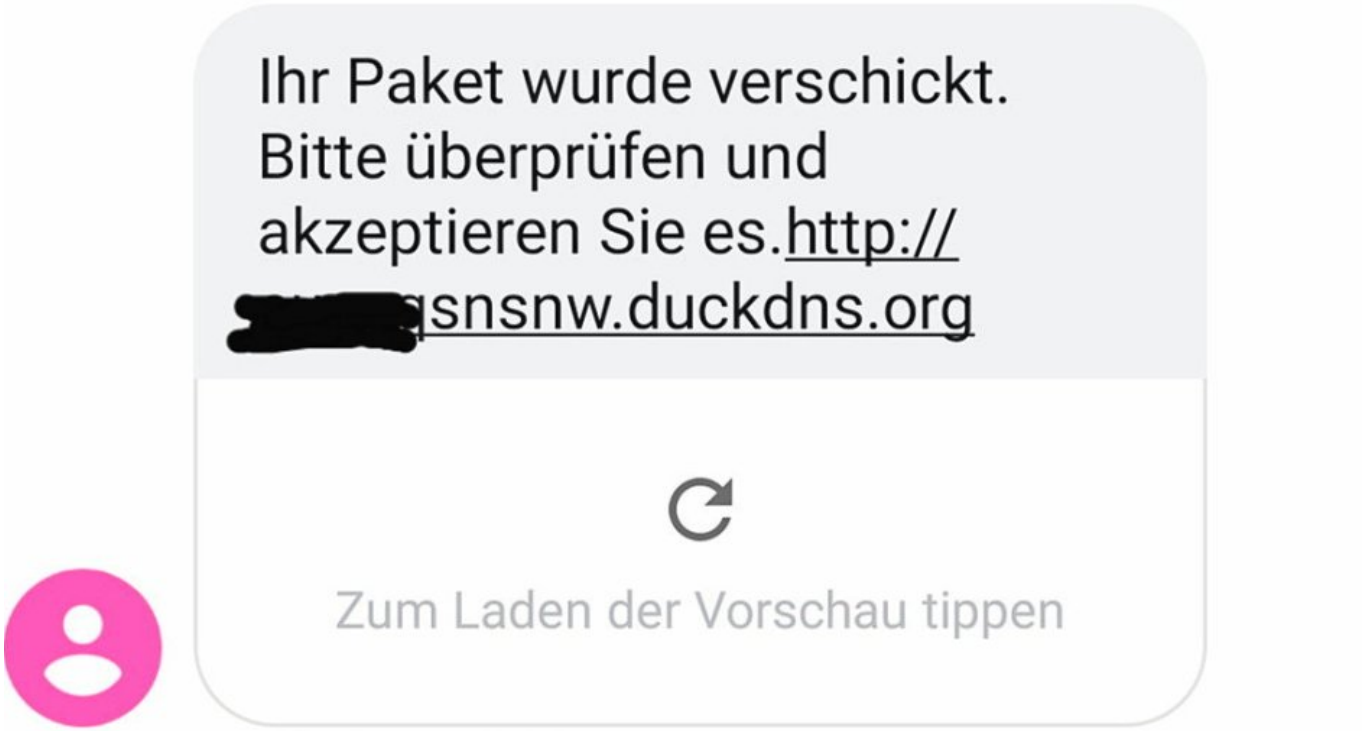
WAZ FUNKE Medien Nordrhein-Westfalen

CYBERKRIMINALITÄT

Hackerangriff aus China: Gefährliche Paketzustellung-SMS WAZ+

05.04.2021, 17:36 | Lesedauer: 5 Minuten

Michael Koch



Derartige Kurznachrichten landen derzeit massenhaft und bundesweit auf Handys oder Smartphones. Den Link darf man auf keinen Fall anklicken!
Foto: Polizeidirektion Flensburg / Polizei

HAGEN/MENDEN. **Massenhaft erhalten Menschen dubiose SMS zu Paketzustellungen. Der IT-Forensiker Karsten Zimmer erforscht die Gründe und hat deutliche Warnungen.**

Die Masche ist so perfide, weil der Anlass so alltagstauglich scheint. Eine SMS oder eine Whatsapp landen auf dem Smartphone, angeblich mit einem Link zur Online-Nachverfolgung einer Paketzusendung. Hatte ich was bestellt? Erwarte ich tatsächlich ein Paket? Gerade jetzt, wo in Lockdown-Zeiten ohnehin viel mehr online bestellt wird, kann schon allein diese Neugierde dazu verleiten, auf diesen Link zu klicken. Doch die Polizeibehörden in der Region warneneindringlich davor: Schad-Software könne das Smartphone mit dem Klick auf den Link befallen.

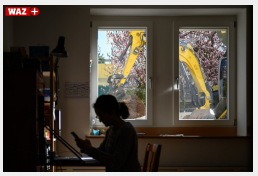
IT-Forensiker war auch im Missbrauchs-Komplex Lügde eingesetzt

Der Mendener Karsten Zimmer beschäftigt sich intensiv mit dem Problem. Er ist IT-Forensiker, quasi ein Gerichtsmediziner in Sachen Computer und Netzwerke. Er war schon für das Bundeskriminalamt und die Landeskriminalämter tätig und jüngst auch an der Auswertung des Datenmaterials im Kindermissbrauchsskandal von Lügde beteiligt. Jetzt beschäftigt er sich gemeinsam mit einem Professor der Fachhochschule Mittweida mit den Hintergründen dieser gefährlichen Kurznachrichten.

Die ersten Erkenntnisse: Sie beruhen offensichtlich auf einem chinesischen Hackerangriff auf Server, insbesondere auch auf Mail-Server. Und gerade die in der Pandemie viel diskutierte Corona-Warn-App und die Luca-App könnten nach Ansicht von Karsten Zimmer ausgenutzt werden, um ganze Bewegungsprofile zu erstellen. „Dahinter steckt die chinesische Hackergruppe ‚HAFNIUM'", sagt Karsten Zimmer im Gespräch mit dieser Zeitung. „Diese Cyberkriminellen arbeiten meist auf staatlicher Ebene."

CORONA

Corona-Krise: Internet-Kriminelle kapern das Home-Office



Anfang März hatte das Bundesamt für Sicherheit in der Informationstechnik auf mehrere Schwachstellen in verschiedenen Versionen des Betriebssystems Microsoft Exchange Server hingewiesen. Tausende Server allein in Deutschland seien so angreifbar. Microsoft selbst hat auch zu einem Update aufgerufen, um die Angriffslöcher zu stopfen. „Doch auch nach dem offiziellen Update-Patch von Microsoft sind noch viele Server infiltriert", sagt Karsten Zimmer.

Chinesische Hackergruppe hat E-Mail-Verkehr abgegriffen

Der Mendener und sein Mitstreiter haben Server von durch den Hackerangriff betroffenen Unternehmen analysiert. „Uns ist aufgefallen, dass es seit einigen Wochen verstärkt zur Versendung von Textnachrichten per SMS an Mitarbeiter und Kunden dieser betroffenen Unternehmen kommt", sagt Zimmer. Auch die Telekom habe in einem Sondertreffen mit dem IT-Forensiker bestätigt, dass der SMS-Versand extrem zugenommen habe. „Immer wieder wurden angebliche Links versendet, um Pakete zu tracken."

Seine These: Die chinesische Hackergruppe hat den E-Mail-Verkehr und Kundendaten abgegriffen und daraus die Handynummern gezogen. „Auch wenn jemand vielleicht nicht mit der Handynummer im Kundenverzeichnis steht: Es reicht, wenn in einer Mail vielleicht die Handynummer auftaucht."

Corona-App und Luca-App können missbraucht werden

Auch die Corona-Warn-App der Bundesregierung, aber auch privaten Apps zur Kontaktnachverfolgung wie Luca, könnten die Hacker missbrauchen, wenn Nutzer den vermeintlichen Paketlink anklickten, vermutet Karsten Zimmer. „Dabei werden nicht die Apps selbst gehackt. Und auch wird nicht der gesicherte Bereich der Apps – Sandbox genannt – abgegriffen, sondern die Kommunikation der Apps mit dem Smartphone, wenn es um den derzeitigen Standort geht." Die Apps sollen ja gerade verschlüsselt feststellen, wo man sich befindet und der IT-Forensiker befürchtet, dass so Hacker auch komplette Bewegungsprofile erstellen könnten.

IT-Forensiker Karsten Zimmer aus Menden.
Foto: Corinna Schutzeichel / WP

Das könne soweit gehen, dass die Hacker feststellen könnten, ob sich ein Mitarbeiter im Homeoffice befinden, wo die IT-Bereiche, mit denen man arbeite, meist noch weniger gegen Cyberangriffe geschützt seien. „Ich will nicht gegen die Corona-Warn-App oder die Luca-App sprechen", sagt der Mendener, wohlwissend, dass er in der aktuellen Situation der Pandemie ein sensibles Thema anspricht. „Aber man muss sich dessen bewusst sein."

Unternehmen sollten auf Auffälligkeiten achten

Die Unternehmen selbst merkten zunächst gar nichts davon, dass ihre Server von dem Hackerangriff seit Jahren betroffen seien, so Karsten Zimmer. Von dieser Sicherheitslücke (Exploid) seien die Betriebssysteme Windows Server 2010 bis einschließlich 2019 betroffen: „Deshalb sollten alle genau hinschauen, ob sie Rückmeldungen bekommen, dass es Auffälligkeiten gibt, dass etwa verstärkt Mitarbeiter oder Kunden diese Paketlink-SMS erhalten haben. Dann solle man sofort IT-Experten einschalten, um das Ganze forensisch zu untersuchen.

Für alle Bürger hat Karsten Zimmer eine noch viel einfachere Mahnung, die ähnlich klingt wie die der Polizei: „Ich warne ausdrücklich vor dem Öffnen der WhatsApp- und SMS-Nachrichten und vor allem vor der Linkbestätigung."

>> HINTERGRUND: Sofort die Verbindung zu mobilen Daten kappen

- Laut Polizei Hagen sind derzeit **Android-Smartphones** eher von den kriminellen SMS betroffen als I-Phones. Auch dort landeten zwar die Kurznachrichten, jedoch lade sich die Datei nicht auf das Betriebssystem. Ein künftiger Befall könne jedoch nicht ausgeschlossen werden.

- Die Polizei rät: Sie warten tatsächlich auf ein Paket? Dann informieren Sie sich ausschließlich **direkt auf der Internetseite des Händlers** über die Sendung.

- Entsprechende SMS sollte **man löschen**, aber nach Möglichkeit daran denken, vorher einen **Screenshot der Nachricht zu machen**, mit Hinweis auf die Absender-Rufnummer. Wer doch auf den Link geklickt habe, solle keinesfalls Daten preisgeben und keine Updates oder Installationsaufrufe bestätigen.

- Falls doch **bereits ein Installationsprozess** laufe, solle man sofort die Verbindung zum Mobilfunknetz und zum WLAN trennen – etwa durch Einschalten des Flugmodus. Und: Auf jeden Fall bei der Polizei melden.

KOMMENTARE ›

Mehr Artikel aus dieser Rubrik gibt's hier: Wirtschaft