Praxistipp Datenschutz 01 | 2021

Verschlüsselungstrojaner ignorieren bedeutet Lebensgefahr für das Unternehmen!

Es passiert derzeit immer öfter: Stellen Sie sich vor, Sie erhalten eine Mail von einem Geschäftspartner oder Dienstleister. Darin soll vorsorglich darüber informiert werden, dass durch einen Trojaner-Angriff Dateien kompromittiert wurden. Da Sie mit dem Versender der Nachricht in direktem Geschäftsverkehr stehen, können Sie ab sofort vom jeweiligen Trojaner betroffen sein.

Warum können Sie betroffen sein? Vor allem der Verschlüsselungs-Trojaner Emotet versucht nicht mehr wie früher, ein System so rasch wie möglich lahmzulegen. Ziel ist es heute, möglichst viele Kontakte und Informationen aus dem laufenden Geschäftsmodell zu ziehen, um andere Unternehmen über täuschend echte Mails ihrerseits zu infizieren. Wenn Sie Geschäftspartner des Unternehmens sind, können Sie ebenfalls betroffen sein.

Was ist direkt zu tun? Als Erstes müssen Sie überprüfen, was genau an Informationen gesendet wurde. Je genauer die Informationen sind, desto geringer kann in der Folge das Risiko sein, dass Sie falsch gehandelt haben. Hier wird der Ablauf des Angriffs beschrieben und ob personenbezogene Daten abgegriffen worden sein können.

Gegebenenfalls müssen Sie der Meldepflicht nachkommen! Ist das der Fall, müssen Sie Ihrerseits Ihre Geschäftspartner darüber informieren, dass Mails von Ihnen kompromittiert sein könnten. Außerdem müssen Sie prüfen, ob dadurch eine Meldepflicht an die Aufsichtsbehörde nach Art. 33 DSGVO durch Sie erfolgen muss. Normalerweise bedeutet die Mail jedoch nur, dass Sie über den Vorfall bei Ihrem Geschäftspartner oder Dienstleister informiert sind und entsprechende Vorkehrungen treffen sollten.

Was ist indirekt zu tun? Angenommen, der Angreifer, der bei Ihrem Geschäftspartner oder Dienstleister den Trojaner platziert hat, ist jetzt auch an Informationen über Ihr Unternehmen gelangt. Ab sofort müssen Sie damit rechnen, dass Sie und Ihr Unternehmen ganz oben auf der Liste der Angreifer stehen. Es gilt, angemessene Vorkehrungen zu treffen, dass ein jetzt erfolgender Angriff verlässlich erkannt und abgewendet wird. Sonst ist Ihr Unternehmen das nächste Opfer des Erpressungstrojaners. Die Bedrohung zu ignorieren, bedeutet Lebensgefahr für Ihr Unternehmen.

So könnte der Angriff abgelaufen sein Immer häufiger passiert es, dass eine völlig unverfänglich erscheinende E-Mail aus einem real existierenden Geschäftskontakt durch den Trojaner verseucht ist. Das kommt daher, dass die Angreifer durch den Trojaner möglichst lange auf dem System des übernommenen Unternehmens sein wollen, um möglichst viele echte Geschäftskontakte ausfindig zu machen. Denn auch die Angreifer wissen, dass mit 08/15-Mails, in denen beispielsweise eine hohe Geldsumme versprochen wird, heute

niemand mehr auf einen entsprechenden Link klickt. Zumindest hoffentlich. Daher versuchen sie, über real erscheinende Mails, wie sie tagtäglich im Geschäftsverkehr vorkommen, den Verschlüsselungstrojaner weiterzugeben.

Was könnte das für Ihr Unternehmen bedeuten? Alle beschäftigten Personen, die mit dem kompromittierten Geschäftspartner oder Dienstleister im Geschäftskontakt stehen, müssen sofort über den erfolgten Angriff informiert werden. Jede weitere Mail von diesem Geschäftspartner oder Dienstleister muss besonders kritisch betrachtet werden. Schon eine geringe Abweichung vom üblichen Prozess, beispielsweise eine plötzliche Fehlermeldung in einer Word-Datei oder die Aufforderung, ein Makro zu aktivieren, ist ein starkes Indiz dafür, dass es sich auch hierbei um eine verseuchte Mail handelt. Wird dieser Aufforderung Folge geleistet, hat dann auch Ihr Unternehmen den Trojaner in seinem System.

Alle Möglichkeiten durchspielen und angemessen informieren Es kommt nun darauf an, möglichst schnell alle Personen zu informieren, die mit dem kompromittierten Unternehmen in Kontakt stehen. Der Angriff kann aber noch perfider funktionieren. Beispielsweise dann, wenn bei Ihrem Geschäftspartner weitere Geschäftskontakte Ihres Unternehmens hinterlegt sind. Dann kann es nämlich passieren, dass die Angreifer auch deren Geschäftsdaten nutzen, um dort über fingierte Mails verseuchte Dateien zu platzieren. Es ist also möglicherweise nicht allein damit getan, auf die Infektion beim Geschäftspartner oder Dienstleister hinzuweisen, es muss auch analysiert werden, welche weiteren Kontakte betroffen sein könnten.

Jetzt heißt es, angemessen zu sensibilisieren! Spätestens jetzt ist es höchste Zeit, alle beschäftigten Personen, die über ein Mailkonto verfügen und demzufolge Adressat eines möglichen Angriffs sind, mit den Risiken und der üblichen Vorgehensweise der Trojaner so gut wie möglich vertraut zu machen, Stichwort Mitarbeiterschulung. Diese Schulung kann unter Pandemie-Bedingungen in der Regel nicht persönlich durchgeführt werden. Für diesen Fall ist entweder eine Schulung über ein Videokonferenzsystem oder eine Schulung als MP4-Video zu wählen. Wichtig ist, so rasch wie möglich alle Personen zu erreichen, die eine solche kompromittierte Mail erhalten können, damit sie im Ernstfall richtig reagieren.

Vergessen Sie die IT nicht! Nicht vergessen werden darf an dieser Stelle die IT. Stellen Sie sicher, beispielsweise PCs nicht so zu konfigurieren, dass eine Infektion sofort auf alle anderen PCs überspringen kann. Hier gilt es, Vorkehrungen etwa in Form einer Firewall zwischen den Systemen zu treffen. Weiterhin sollten für jedes System eigene Admin-Passwörter gewählt werden. Ein Master-Passwort für alle IT-Systeme wäre quasi der Generalschlüssel für den frisch eingedrungenen Datendieb. Es ist also jetzt eine gute Gelegenheit, die aktuellen Einstellungen zu überprüfen und bei Bedarf anzupassen.

Rechtsquellen zum Nachlesen

Meldepflicht: Art. 33 DSGVO

Schutzverletzungen: Art. 4 Abs. 12 DSGVO

Schulungspflicht: Art. 39 Abs.1 lit. a DSGVO

Alle Praxistipps gibt es auf team-datenschutz.de

Lösungen zu Schulungen zur Vermeidung von Trojanern und zu den richtigen IT-Einstellungen? Fragen Sie uns.

Persönliche Beratung, passgenaue Umsetzung. Mit *Team* Datenschutz sind Sie in Sachen Datenschutz und Informationssicherheit einen Schritt voraus.

Hier schreibt Eberhard Häcker, Externer Datenschutzbeauftragter, Datenschutzberater, Fachautor und Kongressredner, Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und der HäckerSoft GmbH (Datenschutz-Software DATSIS und Lernplattform Optilearn.de). Er ist überzeugt, „den spannendsten Beruf der Welt“ zu haben, denn Datenschutz unter der DSGVO ist „wie die Besiedlung Amerikas – weißes Land, das es zu entdecken und sinnvoll zu füllen gilt“. (Eberhard Häcker)