EV 10.3.17

Ausgespäht, erpresst und ausgenommen

Internet-Kriminelle legen Betriebe lahm

HANNOVER/MÜNSTER (dpa/mel). Plötzlich waren alle Computer gesperrt. Bei dem mittelständischen Unternehmen aus Niedersachsen lief nichts mehr. Im Februar wurde es Opfer einer Schad-Software (Ransomware), die Computer blockiert und ihre Nutzer erpresst. Um wieder an ihre Daten zu kommen, zahlte die Maschinenbau-Firma „Lösegeld" in Form der Internetwährung Bitcoins. Der Wert: Mehrere Hundert €. Die Entschlüsselung funktionierte – aber nur teilweise, so dass das Unternehmen auf seinen Schäden sitzen blieb. Es gab Verluste im sechsstelligen Euro-Bereich.

Es ist einer der jüngsten Fälle von Internet-Kriminalität. 2016 waren mehrere Attacken auf Kliniken in NRW bekannt geworden, die sich nach Cyber-Angriffen freikaufen mussten.

„Norddeutschland ist derzeit offensichtlich das Ziel einer größeren Betrugswelle", so Tilmann Brunner, Außenwirtschaftsexperte der Industrie- und Handelskammer (IHK) in Hannover. Auch das LKA bestätigt, dass Cyber-Kriminelle immer häufiger Schwachstellen in Software und Geräten ausnutzen, um IT-Systeme zu attackieren und Firmen zu erpressen. Mit infizierten E-Mails wird bei derartigen Angriffen oft Software in die Rechner geschleust.

Die schlechte Nachricht: Sogenannte Erpresser-Software kommt immer ausgefeilter daher und ist auf regelrechten Marktplätzen in den verborgenen Ecken des Internets („Darknet") einfach zu bekommen. Laut einer Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) war im April 2016 jedes dritte deutsche Unternehmen in den vorangegangenen sechs Monaten von Ransomware betroffen.

Die rasante digitale Vernetzung macht viele Unternehmen angreifbar. Aktuell ist es vor allem die sogenannte Chef-Masche, mit der die Gauner auf Beutezug sind. Bei der auch „CEO-Fraud" (Vorstands-Betrug) genannten Taktik geben sich die Kriminellen als Vorstand oder Geschäftsführer aus und weisen Mitarbeiter der Finanzabteilung per täuschend echter Mail an, große Geldbeträge für angeblich wichtige Geschäfte zu überweisen. Die unter falschen Namen eröffneten Konten werden sofort leergeräumt.

„Von diesen Chefmails waren auch Firmen in unserem Kammerbezirk bereits betroffen", bestätigt Guido Krüdewagen, Sprecher der IHK Nord Westfalen in Münster. Die Betrüger seien sehr gut über die Struktur, Hierarchieebenen und Absatzmärkte des Unternehmens informiert, weil sie im Vorfeld E-Mail-Konten hackten und die Unternehmen sorgfältig ausspähten. Und: „Die Täter verwenden E-Mail-Adressen, die nicht nur auf den ersten Blick genauso aussehen wie zum Beispiel die echte Adresse des Geschäftsführers". Die IHK rät den Unternehmen zusätzliche Sicherheitsmaßnahmen zu vereinbaren, „etwa, dass der Chef in jedem Fall noch einmal anruft."

„Das Geschäftsmodell der Cyber-Erpressung wird sich in mehrere Richtungen weiterentwickeln", vermutet Raimund Genes von der Cyber-Sicherheitsfirma Trend Micro. „Denn mit der Drohung, die Temperatur einer Anlage zu manipulieren oder gleich eine ganze Produktionsstraße außer Betrieb zu setzen", lasse sich noch mehr Lösegeld erpressen.