

## Cybercrime in Deutschland – die zentrale Bedrohung

Am 30.09.2020 wurde der „Cybercrime Bundeslagebild 2019“ des BKA veröffentlicht. Wie wir hieraus, durch die Medien und durch unser direktes Umfeld, entnehmen können, ist und bleibt Ransomware die größte Bedrohung in der IT. „Im Jahr 2019 entstand ein Schaden von circa 102,9 Mrd. Euro durch Cyberangriffe auf Wirtschaftsunternehmen.“

Das BKA spricht darüber, dass aktuell über 1 Milliarde Malware-Familien festgestellt wurden. Jedoch kann die Anzahl der Malware-Familien nicht exakt beziffert werden. Der Grund dafür liegt in der extremen Dynamik von Cybercrime – jeden Tag werden dutzende neue Varianten von Malware-Familien identifiziert.

### Malware – und seine tausend Gesichter

Wenn wir uns näher mit dem Thema Malware beschäftigen, müssen wir uns zuerst die Fragen stellen: Was ist Malware? Das BKA definiert Malware folgendermaßen:

Unter dem Begriff Malware versteht man alle Programme, welche schädliche Funktionen auf einem IT-System ausführen.

Zu diesen maliziösen Funktionen gehören u.a.

- Ausspähen und Weiterleiten von Account-Daten wie Usernamen und Passwörtern,
- Manipulation bzw. Zerstörung von Daten,
- illegitime Nutzung von Rechenleistung zum Kryptomining,
- Verschlüsseln von Daten,
- Einbindung in ein Bot-Netz und zum Missbrauch für DDoS-Angriffe,
- missbräuchliche Fernsteuerung eines fremden IT-Systems.

Das BKA berichtet, dass ein Großteil von Cyberstraftaten mittels Malware begangen werden. Diese dringen in fremde Systeme ein und führen dort eine Vielzahl an schädlichen Funktionen aus. Dabei kann die Distribution von Malware-Familien auf die unterschiedlichsten Weisen erfolgen, jedoch sind die am häufigsten ausgenutzten Eintrittsvektoren in ein fremdes System, infizierte Anhänge von Spam-Mails.

Ein Trend, der sich in den letzten Jahren abzeichnet, ist die zunehmende Professionalisierung der Malware-Programmierer und des sog. Malware-Cryptings: Sowohl der eigentliche Schadcode als auch dessen Verschlüsselung / Verfremdung (Crypting) entwickeln sich weiter und werden komplexer. Ziel von Cyberkriminellen ist die Verbesserung der sog. Obfuskationsfähigkeit (Verschleierung vor Sicherheitsmechanismen, wie z.B. Antiviren-Scannern) der Schadsoftware, um möglichst lange vor Sicherheitssystemen unentdeckt zu bleiben.

### Ransomware – die digitale Erpressung

Ist Ransomware etwas anderes? Der Trend von zielgerichteten, hochprofessionellen Ransomware-Angriffen auf Unternehmen setzt sich laut dem BKA fort. Die Intensität dieser Angriffe und die dadurch entstehenden Auswirkungen nehmen permanent zu. Doch was versteht man unter Ransomware? Zusammengefasst definiert das BKA Ransomware folgendermaßen:

**Ransomware verschlüsselt die Daten eines digitalen Systems und führt in vielen Fällen zur Sperrung anderer, in einem Netzwerk erreichbarer Endgeräte.**

Es gibt unterschiedliche Arten von Ransomware:

- a. Erpressungssoftware, die tatsächlich keine Verschlüsselung der Festplatte durchführt, sondern durch eine Manipulation lediglich den Zugriff auf das System versperrt. Die wohl bekanntesten Ausprägungen sind Schadprogramme, bei denen bekannte Namen und Logos von Sicherheitsbehörden (bekannte Beispiele sind z.B. der sog. BKA-Trojaner und der GVV-Trojaner) missbraucht werden, um der kriminellen Zahlungsaufforderung einen vermeintlich offiziellen Charakter zu verleihen.

- b. Sog. Krypto-Ransomware, welche die Daten auf den infizierten Endsystemen und aktuell auch mittels netzwerkverbundener Systeme (Server, Storage etc.) verschlüsselt. Diese Variante birgt für den Betroffenen ein sehr hohes Schadenspotenzial, da die genutzten Verschlüsselungen nicht in allen Fällen überwunden werden können. Die Zahlung des geforderten Lösegelds führt darüber hinaus häufig nicht zur Entschlüsselung des infizierten Systems.
- c. Ein sog. Wiper weist gegenüber einer „herkömmlichen“ Ransomware einen entscheidenden Unterschied auf: Die Funktionalität zum Entschlüsseln und Wiederherstellen von Daten auf einem System ist nicht vorhanden – die Daten werden somit unbrauchbar und irreversibel zerstört. Selbst nach der Bezahlung des Lösegeldes können die Daten nicht wiederhergestellt werden.

Ransomware-Angriffe auf Unternehmen besitzen das Potenzial, existentielle Bedrohungen auszulösen.

### Erhöhtes Schadenspotenzial durch Double Extortion

Um die Betroffenen unter verstärkten Druck zu setzen, die Lösegeldsummen zu zahlen, ist seit 2019 eine weitere Facette bei den Angriffen zu erkennen. Beim sog. Double Extortion verschlüsseln die Ransomware-Akteure nicht mehr nur die IT-Systeme ihrer Ziele, sondern leiten vor der Kryptierung sensible Daten aus und drohen damit, diese zu veröffentlichen. Hiermit ist nicht nur die Verfügbarkeit der kryptierten Daten bedroht, sondern auch deren Vertraulichkeit und damit die Reputation des Opfers.

Hiermit haben im Jahr 2019 die Entwickler der Ransomware „Maze“ begonnen und dieser Modus wurde von weiteren Akteuren wie z.B. den Gruppierungen hinter den Ransomware-Familien Nemty und Sodinokibi übernommen. Aufgrund des lukrativ empfundenen Geschäftsmodells ist anzunehmen, dass weitere Täter diesen Modus Operandi übernehmen werden.

### Angriffe auf Wirtschaft und KRITIS

„Drei von vier Unternehmen wurden 2019 Opfer von Cyberkriminellen – 2017 nur jedes zweite.“

Täglich steigt die Anzahl von Cybercrime betroffenen Unternehmen signifikant. Unternehmen sehen sich einer großen Bandbreite an Cyberangriffen ausgesetzt. Angefangen bei der Ausspähung von sensiblen Daten, ihrer missbräuchlichen Veränderung, Manipulation von Webseiten, die Infizierung mit Schadsoftware, bis hin zur Verschlüsselung oder Zerstörung von Daten. Durch eine zunehmende Professionalisierung der Täterseite verschärft sich diese Situation zunehmend.

Dabei stehen laut dem BKA kleine und vermehrt große private Unternehmen, aber auch öffentliche Einrichtungen verstärkt im Fokus von Cyberkriminellen. Das BKA geht, in Anbetracht der im „Cybercrime Bundeslagebild 2019“ geschilderten Entwicklungen, von einer Zunahme der Cyberangriffe auf KRITIS aus.

### Zusammenfassend möchte ich das BKA zitieren:

„Von allen hier dargestellten Phänomenen hat Ransomware das in Summe höchste Schadenspotential für Unternehmen, öffentliche Einrichtungen, Behörden und Kritische Infrastrukturen. Eine Infektion mit Ransomware und eine damit zusammenhängende Verschlüsselung des Systems kann für jede Art von Unternehmen zu massiven und kostenintensiven Geschäfts- bzw. Funktionsunterbrechungen führen.“

<b>INNEO</b> <sup>®</sup> Händlerinformation <b>That's IT.</b>	
INNEO Solutions GmbH · inneo@inneo.com · www.inneo.com	
Deutschland: Rindelbacher Straße 42 73479 Ellwangen Telefon: +49 (0) 7961 890-0 Fax: +49 (0) 7961 890-177	Schweiz: Ruchstückstrasse 21 CH-8306 Brüttsellen Telefon: +41 (0) 44 805 1010 Fax: +41 (0) 44 805 1011