BEST GRUPPE

BEST Aktuell

WannaCry-Attacke: "Dieser Angriff ist ein Weckruf"

Düsseldorf, 15. Mai 2017 – Ende letzter Woche schlugen Cyber-Kriminelle erneut zu – und das gleich weltweit. Über 100 Länder waren betroffen. Zigtausende Computer wurden Opfer der Schadsoftware "WannaCry".

Der Name war sicher nicht wahllos ausgesucht. Vor ihrem Rechner sitzend, waren unzählige Nutzer, ganze Firmen, den Tränen nah`. Das Programm, das die Daten befallener Rechner und Netzwerke verschlüsselt, „erbat" Lösegeld. Erstmalig in der Geschichte der noch recht jungen deutschen Cyberkriminalitäts-Abwehr äußerten Fachleute den Gedanken, zu zahlen wäre nicht die schlechteste Wahl. Rund 300 Euro in der Digitalwährung Bitcoin gab den Code zur Entschlüsselung preis. Das Erschreckende daran war also weniger die Schadenhöhe, sondern vielmehr die damit als möglich bewiesene, stündlich und millionenfache Verbreitung. Vor allem betroffen: Unternehmen, Behörden und Privatpersonen. Sogar vor Krankenhäusern machten die Erpresser keinen Halt. Und auch hoch gesicherte Dienstleister wie Telefónica in Spanien oder die Deutsche Bahn fielen ihnen zum Opfer.

Der entscheidende Unterschied zu bisherigen Attacken durch Trojaner: Üblicherweise muss der Nutzer einem Trojaner und ähnlicher Schadsoftware z.B. über einen präparierten Link oder den Besuch einer bestimmten Website die „Tür" zu seinem Computer bzw. Netzwerk öffnen. Bei „WannaCry" erfolgt die Verbreitung nach einer initialen Infektion ohne dass der Nutzer noch etwas tun muss.

Laut Einschätzung der europäischen Ermittlungsbehörde Europol erreicht Cyber-Kriminalität mit der aktuellen Attacke ein "beispielloses Ausmaß". Auch das Bundeskriminalamt BKA in Deutschland spricht von einem schwerwiegenden Angriff.

Die Cyber-Experten der BEST GRUPPE nehmen Unternehmensrisiken unter die Lupe. Sie erfassen und bewerten die ganz individuellen Risiken - soweit erforderlich mit Unterstützung externer Experten. Dabei geben sie nicht nur wertvolle Hinweise, passend zu den technischen Gegebenheiten, sondern werfen auch einen Blick auf Organisationsstrukturen sowie die Erhöhung der Sensibilität von Mitarbeitern. Darauf aufsetzend erfolgt die Ermittlung der optimalen Lösung, um das wirtschaftliche Restrisiko aus dem Unternehmen „auszulagern". Im Falle eines Falles besteht 24 Stunden an 365 Tagen im Jahr der Zugriff auf ein Team von IT-Sicherheitsspezialisten, Forensikern, Marketingfachleuten und Anwälten.