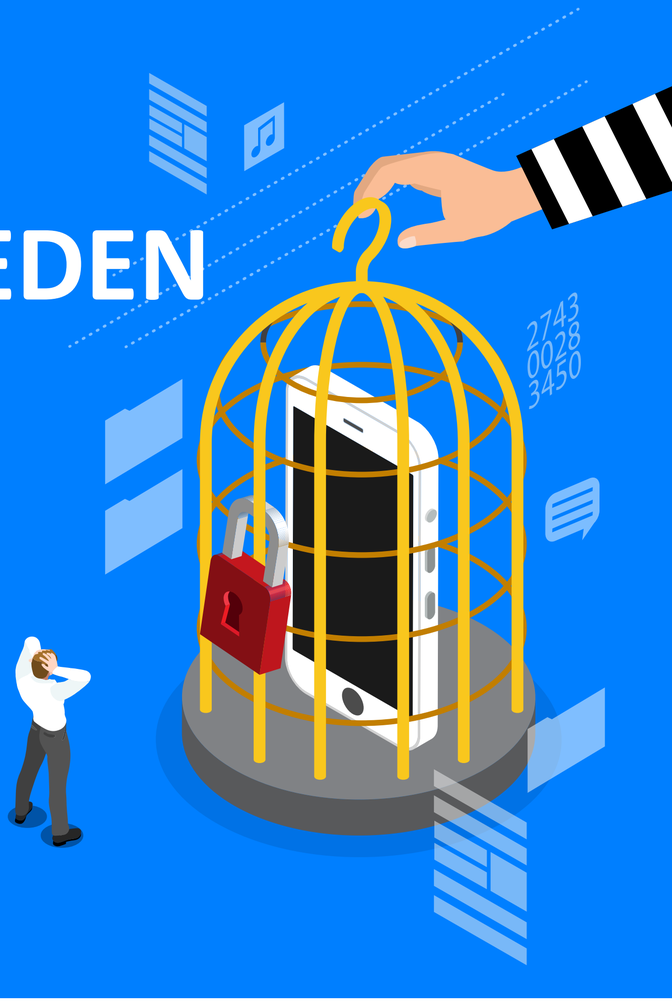
MOBILE
RANSOMWARE

VERABSCHIEDEN SIE SICH VON IHREN DATEIEN



Ransomware verschlüsselt Ihr mobiles Endgerät sowie die darauf gespeicherten Daten und fordert die Bezahlung eines Lösegeldes.

WIE VERBREITET SIE SICH?

Besuch kompromittierter Webseiten.

Herunterladen von gefälschten Versionen legitimer Apps.

Klicken auf bösartige Links und Anhänge in Phishing-E-Mails.

WAS SIND DIE RISIKEN?

Sie müssen Ihr Gerät eventuell auf die Werkseinstellungen zurücksetzen, all Ihre Daten gehen verloren.

Ein Angreifer kann unbegrenzten Zugriff auf Ihr Gerät erhalten und Ihre Dateien/Daten mit Dritten teilen.

WAS KÖNNEN SIE TUN?

Sichern Sie Ihre Daten regelmäßig und halten sie all Ihre Apps und Ihr Betriebssystem auf dem aktuellen Stand.

Erwerben Sie Ihre Apps nicht in unbekannten App-Stores oder Stores von Drittanbietern.

Falls verfügbar, installieren Sie eine Mobile-Security-App, die Sie warnt, wenn Ihr Gerät kompromittiert wurde.

Setzen Sie im Umgang mit E-Mails und Webseiten Ihren gesunden Menschenverstand ein: Öffnen Sie keine verdächtigen oder unglaubwürdigen E-Mails, Links oder Anhänge.

Geben Sie niemandem Administratorrechte für Ihr Gerät.

Zahlen Sie das Lösegeld nicht. Sie finanzieren damit Kriminelle und ermutigen diese, ihre illegalen Aktivitäten fortzusetzen.

EUROPOL EC3 European Cybercrime Centre

Bundeskriminalamt

#MobileMalware