

* Connecting to database at 172.33.326.17.....
 * User ID:
 * Password:
 Link established
 * Downloading data.....
 36663 kb of 256002kb
 * FATAL EXCEPTION: CONNECTION TERMINATED

YOUR PHONE IS INFECTED. YOU HAVE 96 HOURS TO RECOVER FILES IN ORDER TO PREVENT THE LOSS OF YOUR DATA. ALL FILES WILL BE DELETED AND YOUR PHONE WILL BE LOCKED. IF YOU DO NOT PAY THE RANSOM, YOUR PHONE WILL BE DELETED AND YOUR LOCATION WILL BE SHARED WITH THE POLICE. IF YOU DO NOT PAY THE RANSOM, YOUR PHONE WILL BE DELETED AND YOUR LOCATION WILL BE SHARED WITH THE POLICE. IF YOU DO NOT PAY THE RANSOM, YOUR PHONE WILL BE DELETED AND YOUR LOCATION WILL BE SHARED WITH THE POLICE.

Enter decryption code:

GDATA

Unternehmen bleiben auch in der aktuellen Corona-Pandemie ein attraktives Angriffsziel für Kriminelle. Da viele Firmen gerade mit wirtschaftlichen Schwierigkeiten kämpfen, steigt das Risiko deutlich, bei einer Ransomware-Attacke enormen finanziellen Schaden zu erleiden. Denn gerade jetzt haben die Lösegeldforderungen das Potential, ein Unternehmen in den Ruin zu treiben. Hinzu kommt: Durch den Umzug ins Homeoffice hat die Komplexität der Netzwerke in vielen Unternehmen zugenommen. Die Sicherheit ist aber nicht in dem gleichen Maße gewachsen, insbesondere wenn etwa der Terminalserver oder Sharepoint frei im Internet verfügbar sind, um die Business Continuity zu sichern.

Gerade kleinere IT-Abteilungen in Unternehmen sind derzeit mit dem Umbau der Infrastruktur für die vermutlich längerfristige Homeoffice-Situation stark eingespannt. Das zieht Ressourcen aus dem wichtigen Bereich der Überwachung und Pflege von der Security-Infrastruktur ab. Cyberangriffe könnten in der derzeitigen Situation noch später erkannt werden als in normalen Zeiten. Die Erfahrungen in der Vergangenheit haben gezeigt, dass es meist deutlich mehr als 180 Tage gedauert hat, bis ein Angreifer im Netzwerk bemerkt wurde.

„Wer von zu Hause arbeitet, sollte immer daran denken, dass der Dienstcomputer mit dem Firmennetz verbunden ist“, warnt Berghoff. Noch kritischer sei es, wenn die Anwender ihren privaten Rechner nutzen, um im Firmennetzwerk zu arbeiten. Denn Privatrechner können nicht einfach durch Gruppenrichtlinien oder andere Maßnahmen der IT zentral abgesichert werden – das Risiko für Infektionen steigt. „Im Homeoffice gelten die gleichen Regeln, wie für die Arbeit im Büro: Keine unbekannten Wechselmedien anschließen, keine verdächtigen Links anklicken, Rechner beim Verlassen sperren und Vorsicht beim Öffnen von Mailanhängen. Denn Phishing-Mails kommen auch im Postfach zu Hause an. Natürlich sollte auf allen Rechnern eine aktuelle Sicherheitslösung installiert sein“, so Berghoff weiter.

G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG
G DATA Campus
Königsallee 178
44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de
Tel.: +49 (0) 234 9762-239
Fax: +49 (0) 234 9762-299