Infoblatt „Ransomware WannaCry"

Sehr geehrte Damen und Herren!

Die Ransomware „WannaCry" legt seit Freitag weltweit Computer lahm und blockiert zahllose Unternehmen und Behörden – nach Angaben von Europol gibt es bereits mehr als 200.000 Betroffene.

In Großbritannien wurden Krankenhäuser, in Spanien der Telekom-Konzern Telefónica, in den USA der Versanddienst Fedex, in Deutschland die Deutsche Bahn und viele andere angegriffen. **Bis jetzt sind 150 Länder betroffen**.

Die Schadsoftware verschlüsselt Benutzerdaten auf einem befallenen Computer und versucht sich dann sowohl im lokalen Netzwerk als auch über das Internet weiter auszubreiten. Ausgenutzt wird dabei eine Sicherheitslücke die von Microsoft bereits im März durch ein Update geschlossen wurde. Betroffen sind daher oft nicht mehr unterstützte Betriebssysteme (Windows XP) und System die nicht regelmäßig aktualisiert werden.

Auf dem befallenen Computer erscheint die Aufforderung **innerhalb von drei Tage 300 US-Dollar (275 EUR) in der Internetwährung Bitcoin zu überweisen.**
Sollte binnen sieben Tagen keine Zahlung eingehen, wird angedroht, dass die verschlüsselten Daten gelöscht werden.

Wahrscheinlicher Angriffs-Vektor für die initiale Verteilung ist aber – wieder einmal – E-Mail!
Auch wenn Virenscanner und Spamfilter eingesetzt werden, kann es immer passieren, dass Phishing-Mails „durchrutschen" und neueste Schadsoftware noch nicht erkannt wird.

Internet-Kriminalität, Phishing, Ransomware etc. ist ein globales Geschäftsmodell mit dem Milliarden umgesetzt werden!
Die Kriminellen investieren daher viel Zeit und Mühe um Sicherheitsmaßnahmen zu umgehen.

Es ist daher wirklich wichtig beim Umgang mit Mails Vorsicht walten zu lassen!

Unser Infoblatt „zum sicheren Umgang mit E-Mails" soll Ihnen dabei helfen „verdächtige Mails" zu erkennen.

Extrem wichtig, um – falls man doch von Ransomware betroffen ist – nicht auf die Erpressung eingehen zu müssen, **ist ein funktionierendes Backup!**
(es garantiert ja trotz Zahlung niemand, dass die Daten tatsächlich entschlüsselt werden und das System danach virenfrei ist).

Franz F. Klein - Informationstechnologie

Web http://www.ffk.co.at
E-Mail office@ffk.co.at

Quellen:
http://cert.at/warnings/all/20170513.html
http://cert.at/services/blog/20170514232126-2007.html
http://derstandard.at/2000057513584/WannaCry-Trojaner-legt-zehntausende-Rechner-in-99-Laendern-lahm
http://derstandard.at/2000057570049/Wannacry-Attacken-Microsoft-kritisiert-NSA-und-Regierung

Franz F. Klein - Informationstechnologie

Web http://www.ffk.co.at
E-Mail office@ffk.co.at