Achtung!
Abzocke per SMS, facebook und LinkedIn

Kaum gemeldet – schon passiert: bei facebook und LinkedIn wurden Millionen von userdaten geklaut! Eine der möglichen Folgen ist bereits zu spüren – SMS mit dubiosen Paketzustell-Inhalten und einem integrierten Link, mit dem man reagieren soll.

BLOß NICHT!

Hierbei handelt es sich um Phishing-Fallen, die dazu dienen, mehr personenbezogene Daten von Ihnen abzugreifen. Entweder durch direkte Eingabe oder durch versteckte Einwilligung in die Installation von Malware auf dem Mobilgerät.

Was ist jetzt zu tun?

Besitzer von Firmenhandys oder anderen mobilen Geräten müssen jetzt besonders aufpassen. Auch wenn die Installation von facebook und LinkedIn bestimmt per Richtlinie in Ihrer Firma untersagt ist, dies aber eventuell nicht ganz eng kontrolliert wird, muss jetzt durch den Verantwortlichen ein update der Anweisung erfolgen. Dies ist dann, beginnend mit dieser News, entsprechend zu dokumentieren.

Welche Folgen hat dies im Zusammenhang der DSGVO?

Sollten über die firmeninternen Mobilgeräte personenbezogene Daten anderer Personen (egal, ob Kunden oder Mitarbeiter) an Unbefugte gelangen, stehen Sie als Verantwortlicher in vollen Umfang in der Pflicht! Dies beginnt mit der Meldung einer Datenschutzpanne bei der Aufsichtsbehörde und der eventuellen Information der Betroffenen und kann mit einem schmerzlichen Bußgeld enden.

Dies wollen wir ja alle vermeiden!