Editorial

Cyber Criminals Target Smartphone

For a long time shining Smartphone world is in the sight of the cyber criminals. The Bochum Safety specialist G-Data have included in the account last year. There appear daily 8225 new defective data for android. These could meet worldwide 88% of all Smartphone because these work with Google management android. However I-Phone and Co is for a long time target of cyber attack.

Smartphone and tablet get developed always more to the middle point of digital life. It is classified by Christian Funk, Manager of German laboratory of Kaspersky. He brings the motivation of the criminals to a simple formula "big target group + prospect of grain = attractive goal." The base is sufficient for all safety persons who actively support the idea of safety, their most recent protection standard after Monday of the last week in the world's biggest mobile phone meet the mobile world congress in Barcelona. Therefore the Czech antiviral specialist Avast calls for attention of the danger with mobile bank business through the Trojan with Demo. "The users can trust at least the App Store as Google Play or Apples App Stores" says Avatas leading threat researcher Nikolas Chrysaidos. However caution is given. "One who uses a mobile banking-App should better exactly test whether these are really verified version is or not."

The German users are completely conscious of the mobile dangers. Above 65% are afraid of virus, Trojans and more of mobile instruments. According to a study of Karpersky Lab more than 80% of German users confess that they do not have even a rough or no overview, which can really attack their data.

For the firms there are further challenges with the mobile data processing specially the danger becomes more when coworkers bring in their own instruments in order to take hold of the firm's data. Nevertheless 56% of the firms in Germany have a clear strategy how and when they want to put in the mobile instrument as per the market researchers of IDC. For that scarcely to be overlooked flow of software solutions promised (to become bound to the growing instrument zoo central and safer to manage.

When in future billions of machines, sensors, automobiles or coffee machines wander about in the Internet of Things (IoT), these also threaten to become the inroad for the cyber criminals. The next caring child of IT safety branch is named therefore IoT.

Experts' advice for mobile safety against cyber attack:

Jens Heider, Manager of Test laboratory's Mobile Safety at Fraunhofer Institute for Safe Information Technology (SIT) gives tips how Smartphone become safe working instrument in firms

- Coworker requires clear rule whether and how business data on Smartphone are permitted to be used.
- Firms should test the insertion of administration software (MDM/EMM) (Mobile Device Management/ Enterprise Mobility Management) in order to be able to carry through in the event of the stipulated rules for the protection of firms.
- The mobile grabbing on the administrative infrastructure as for example Email, databanks, document management should not be forgotten.
- The safety of Apps which processes the firm data must be specially critically tested. The number of these Apps should possibly be held small by which a test remains possibly economical. With this the IT department can arrange with new weak places and safety-lapses. There is an overview on all instruments with the seizing of firm data and the used Apps unalterable.

Anil Kumar Ghosh

Source: VDI nachrichten, 23 February 2018, Nr. 8, Seite 1