Assuring Business Competitive Advantage through Eavesdropping Mitigation

Within a globalized world, which is still struggling to overcome the last financial crisis, there is no longer any space for old fashioned business-ethics. Certain eavesdropping and extraction techniques, readily available after a little research within the Internet, make applications available to those interested in rouges procedures. Techniques that were years ago only available to a very limited circle, mostly state-run intelligence agencies. An increasing number of wrong-doers do not care if they pass the threshold into illegality.

Before touching the subject of eavesdropping on land-line and mobile phones, we need to look at data in general. Important information can be derived, extracted and / or modified from PC's, lap-tops, tablets as well as from PDA's and smart phones. Not to forget those many still existing fax-machines that are not integrated into computers.

Further information can be obtained by ruthless competitors scanning social media like Face book, Twitter and Linked In, only to name a few.

This session will dwell briefly on dangers that are lurking within the Cyber Cloud. As the term Cloud has been promoted extremely strong during the last few years, a great amount of people think that their data really is within a cloud. And as a cloud is difficult to touch, their data will be safe. This is another misconception. Somewhere within this real world – and not the cloud, a server is standing either within a building or shack (maybe in Berlin, the Cayman Island, in Receife, Madrid or another exotic location). This is the reality about the cloud. And this server is subject to several threats.

How is your data secured, who may gain access to it, what happens if the provider runs out of money and is bought-out by someone else? What impact will it have on your data? What enforceable guarantees do you have about the integrity of your data? Which laws apply in this jurisdiction? These are just a few highlights that will be touched.

Coming finally to voice-communications, modern land-line telephones like ISDN in Europe and Asia or their equivalent, T1 in the United States, which are literally computers, will be addressed. With patience and a certain know-how these phone-systems can hacked and manipulated.

And not to forget cheap communications like Skype within the private sector and Voice-over-IP (VoIP) with both private and commercial applications. Wireless LAN and Bluetooth will complete the presentation.

While after one (1) hour listening to this presentation you will not leave this room as an expert for secure communications, your awareness-level will have risen to a point were you will be able to judge what could be done by yourself within your environment. If you find yourself in a rather complex situation, you will have learned how to distinguish a "jack-in-every -trade" from a serious eavesdropping expert that you may entrust in solving your problems.

Werner Preining
Captain, CPP, CMAS
Member of the IT-Security Council since 2000
Member of the CMBCC Council since 2000

Vienna / Austria, January 21st, 2013