The bug in the building saves the management consultant

Ansgar Alfred Huth – Data protection and eavesdropping protection specialist

European managers have learnt how to encrypt their know-how and protect it from outsiders. But now the traditional eavesdrop attack in the inner sanctum of the bosses floor is celebrating a devastating comeback.

Listening devices are becoming more and more powerful, cheap and user-friendly. These days you can buy bugs anonymously at discount prices over the internet. In our high performance society people are much more prepared to use illegal means to gain a competitive advantage. Only a few experts in Europe have skills and specialist equipment to implement successful defence strategies against eavesdroppers.

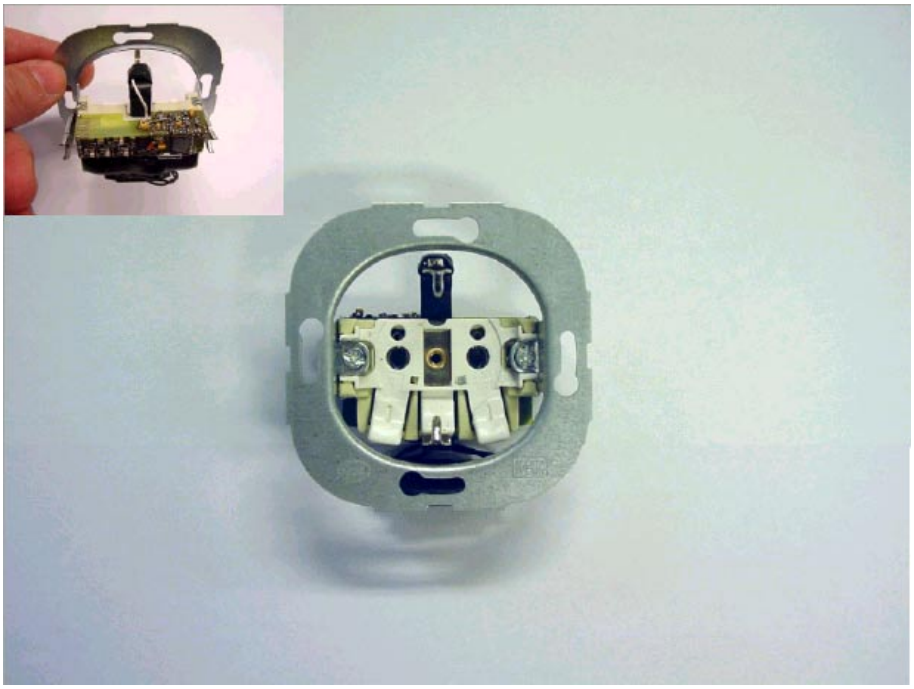
At a time when people have learned to be meticulous about encrypting confidential information and IT security is enjoying top priority in companies, old fashioned bugs are suddenly making a reappearance in the office or private residence. And they are more dangerous than ever. After all the mini spy transmitter has developed terrifically fast in recent years in two different directions. The first direction was predictable. Today's bugs are smaller, more powerful, more user-friendly and more difficult to find than their predecessors. The second, more destructive evolutionary direction taken by these mini traitors couldn't have been foreseen by anyone a few years ago: thanks to the non-controllable internet anyone and everyone can have access to every possible kind of modern spy technology.

high performance bug

Previously spy devices could only be obtained with the right contacts, and at a large cost in time and money, are now offered on the internet – good quality, including operating manual and at discount prices. Disguised as an ash tray, a mobile phone, pocket calculator, biro or electric socket adapter, ready-to-use radio bugs can be bought easily over the world wide web. Some of the guises used by these little information delivery devices are brilliant and with a receiver the size of a cigarette packet, the eavesdropper can hear or record transmitted conversations. And who wouldn't be interested in hearing their competitors plans and weaknesses? Anyone who could read the thoughts of his fellow men would be unbeatable in business (and elsewhere).

With a minimal cost bug bringing such great advantages the readiness to use these illicit information delivery devices has risen immensely in recent years. Especially as the risk of being caught listening is next to none. After all who has an anti eavesdropping system, let alone the knowledge of how to protect business or private life?

According to the manufacturers there are an estimated 500,000 to 1,000,000 eavesdropping devices in private possession in Germany. Anyone who has visited a public security exhibition like “Security” in Essen knows that by far the most popular hall is the one where the listening device suppliers are. A bug the size of a sugar cube only costing a few hundred Euros can eliminate development investment, competitive advantage or even a whole company in no time at all.



AC 220/240 V (110/120) Socket-Transmitter

Placing a listening device is a bit like releasing trojan viruses on the internet. Little presents indicating friendship but triggering a flow of information. Solar pocket calculators, ash trays and other utilitarian objects are the most favoured vehicles for bugs. The briefcase fitted with a transmitter which is left behind in the negotiating room while the owner makes an apparently urgent telephone call, and the mobile phone-come-receiver which enables the unsuspecting negotiating partners conversation to be overheard, can be bought together with an instruction book for a few thousand Euros. A tiny transmitter in the form of a standard socket adapter can take its power from the mains and provide permanent surveillance. And this is only one of the many simple-to-install spy devices the listener can buy off the shelf.

ISDN viruses, telephone bugs, directional microphones, body noise microphones, laser listening devices, computer listening, watching and recording screen displays from a safe distance: all are just a question of money and effort for the criminal users. “Ballpoint pen with built-in high performance bug, that’s 350 Euros please. Can I offer

you anything else?" These words may not be uttered but through the internet the purchase is just as easy.

Ballpoint pen with built-in high performance bug

And our high performance society provides the rewards. Individual employees no longer have the same feelings of loyalty and belonging. Each is out for himself and the person who has more information is sure to be more successful than everyone else. To have a bit more knowledge than other people is a sure way of getting the best deal in all walks of life. Who can deny that? And who wouldn't be tempted?

The danger is therefore real and defence is urgently needed. But only people who have learned about attach can assess the likely weak places and defend themselves. To defend effectively against eavesdropping you have to be able to imagine yourself in the eavesdropper's shoes with his range of possible methods. And only a specialist can do that. A realistic appraisal of the client's situation is only possible with an up-to-date overview of the spying equipment available internationally and constant contact with the manufacturers of eavesdropping defence systems. Only regular contact with developers and manufacturers ensures that you are not outpaced by the increasing electronic and system development, and consequently outplayed by the eavesdropper.

For effective defence it's vital to ensure that the eavesdropper thinks you haven't noticed his attack and therefore won't be counter-attacking. A listener who believes his espionage activities are being investigated, naturally tries to remove and destroy, or at least deactivate the tools of his trade. With standard remote control bugs this means switching off the transmitter unit - as a non-transmitting bug is significantly harder to find than an active one. Bugs of all kinds are the most common espionage method, but the variety of listening systems is only limited by the attacker's imagination and his financial means.

Observation Kit Video Baseballcap

How many people realise that just by analysing compressed HF radiation from a monitor you can reconstruct a live display any text or CAD drawings (in CAD quality of course) on a remote computer screen? This is how a trained TV technician or gifted model-maker can watch a competitor's price calculations live on a modified TV from a safe distance. Of course this compressed radiation is an security loophole for surveillance cameras too. Defending against this kind of spying is totally unspectacular and yet so important. One only has to know about this kind of attack and keep abreast of developments.

What provides effective defence today may be overtaken in a few days, and then, as a completely ineffective defence measure, it represents an even greater potential danger. A businessman with a non-functional defence installation is a sitting target for a listening attack from competitors.

But newness isn't the only criteria for a defence system. For success, quality is important too. The person who believes that they can provide serious protection using a bandwidth detector or field strength meter costing only a couple of hundred Euros might as well share a room with the eavesdropper, that way they both save on system costs and the eavesdropper gets what he wants.

Eavesdropping protection is significantly more expensive than eavesdropping. Whereas the eavesdropper can choose his method or combination of methods, protection involves detecting all possible methods of attack. This requires not just good specialist knowledge but also a set of devices which can check for a wide spectrum of possible espionage methods and systems. A set of anti-listening equipment is not available for less than a five figure sum, then you need specialist knowledge to read the operating manuals.

In Germany research and development over a period of 30 years has led to the production of an eavesdropping protection unit which includes a unique variety of

eavesdropping detection and protection features. And to enable it to be carried inconspicuously into the survey site, it looks just like a normal briefcase. The equipment in the case is kept up to date with software updates and can perform silent room monitoring to detect and locate listening devices, without the listener becoming aware of it. This makes it possible to identify the listener and feed him with false information. Nevertheless 100 percent security does not, and never will, exist. But you can sign up an experienced security partner for your team and fight solidly and effectively against the information theft which is more and more prevalent in our society.

What should you do in suspicious circumstances?

Contact the protection specialist but never from the suspected listening site. It's best if you use a public call box or a telephone/email connection which you would not normally use. For the duration of the telephone conversation turn your mobile phone off, or better still leave it at home or in the car.
Remember that any un-encrypted email can be read and manipulated.

Ansgar A. Huth

Ansgar Alfred Huth – Data protection and eavesdropping protection specialist
63755 Alzenau – Germany
Tel. (06023)918700 huth@spionage.info www.spionage.info