ICT security

COPERNICAN REVOLUTION

Humankind may know thousands of languages but the Internet Protocol (IP) remains almost the only technical data language for global information and communication networking. This uniformity is a huge advantage, but also a major risk. When everything is "brought into line", it is all equally vulnerable to malevolent attacks. That is why a new conceptual focus is recommended today for ultra-sensitive ICT infrastructures.

by Giuliano Otth, President and CEO,
and Heiner Düringer, Senior Vice President, Head of Marketing and Sales

A human organism needs a nervous system to be able to monitor and control all its physical and mental functions as a matter of course. The present-day economy and society are dependent in the same way on a modern infrastructure for information and communication technology (ICT). Comparing ICT with a nervous system makes more sense than one might initially think. ICT is where (global) intelligence is concentrated and where knowledge (of the world) is processed, saved and transferred. With knowledge now in fact the most valuable asset, the value-added process involves not only honest economic players but also criminals large and small as well as genuine warriors. Cyber war is by no means an exaggerated term for this threat.

Cyber war is quite a logical phenomenon as a continuation of human history. What is amazing, however, is that people do not understand or quickly forget the magnitude of the incidents that occur in the economy and society. Examples include the cyber-attack on Estonia or the Stuxnet virus, with which the control systems of industrial plants were deliberately attacked.

This is amazing particularly given the above backdrop of an attack scenario. Anonymous assailants can paralyse entire parts of an infrastructure or government institutions for an extended time by electronic means with no advance warning.

IP as a dangerous master key

Just one standard data language is increasingly winning out above all others in global data networking: Internet Protocol. Consequently, this standard communication protocol is no longer used to network just computers but also millions of control systems, sensors, machines, entire infrastructure installations, etc. Basically, this approach allows one to address, or attack, any active element in the global network from any point of access to the network. A further problem is that most people employ commonly used equipment and user software. That makes attacks even easier. Anyone interested in being and remaining the boss of his own operations has to eliminate this risk with a communication dialect (encryption) incomprehensible to third parties and with defensive walls that are high and extremely effective.

No matter what languages computer users speak, the electronic connection between them is established worldwide with a uniform language known as the Internet Protocol (IP).

Off-the-shelf security not enough

Many a businessman or administrator, CEO or politician believes off-the-shelf security tools that are easy to implement take care of the problem. Unfortunately, new weak points are constantly being revealed and many standard security solutions have known and publicised gaps. The excuse that managers most often give for this high-risk game is this: "More security is out of the question. We couldn't operate efficiently anymore ..."

The solution now is not to compromise but rather to approximate the security approaches of government agencies that may be forced to define certain zero tolerance areas.

Classified information as a model

A zone approach was usually adopted with regard to the confidentiality of data in classic security structures shaped by government agencies with maximum security requirements. The principle is that data and data flows are no longer considered equal but rather classified precisely according to their sensitivity (their value). This approach is based on the security policy of the organisation, which is indispensable in any case. Four (or sometimes only three) classification levels are generally defined: "Top Secret", "Secret", "Confidential" and "Public". The organisation ensures their strict separation by delineating the associated hierarchical security zones (high-security zone, secure zone, trusted zone and public zone). Data with the same classification and protected according to hierarchy moves within the perimeters of these "islands".

Availability and integrity

So, the objective of a well-designed ICT security solution is to protect the data being processed, transferred and saved (particularly the integrity of the data) while at the same time ensuring that the "right" information is available at any time. To this end, the individual zones must be adequately defended by multi-layer defensive walls of technology. The transitional areas between the zones belonging to different hierarchies (perimeters) are the places assailants prefer to attack in the ICT system. Money and effort must be expended in this context. The (types of) data that usually have to be let through are defined precisely so they are available at any time. The entire flow of data is strictly analysed and filtered by specifically configured firewalls and gateways. The zone perimeters are not fixed. Instead, they can be adjusted to constantly changing needs by a user-friendly security management. In zones requiring maximum protection, the connections between geographically separate areas of the same zone (which often pass through public networks) need encryption based on separate hardware.

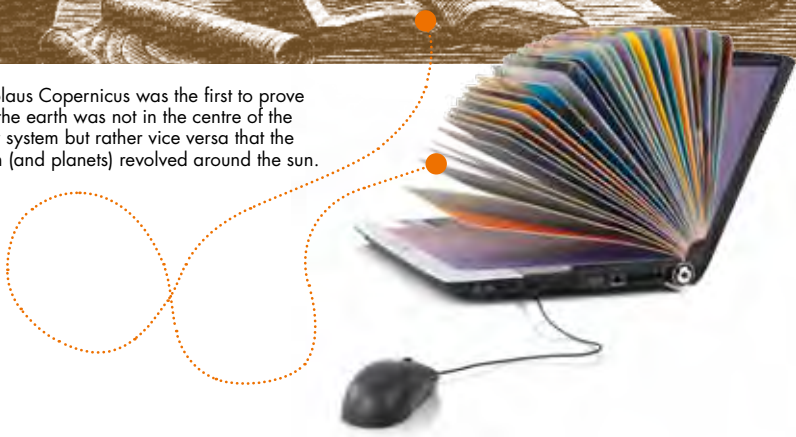
The high-security zone is a special case. Basically, it is not allowed to have a physical network connection to other zones. Consequently, no Internet contact is possible from this zone, for example. Otherwise the zone would not be top secret!

Special technical and organisational knowledge and appropriate technology products are obviously needed to implement these types of ICT security solutions, the designs of which are becoming increasingly customised. Specialised companies such as Crypto AG work in this area according to generally recognised standards, which are supplemented by various special standards stemming from the environment in which organisations with maximum security requirements operate.

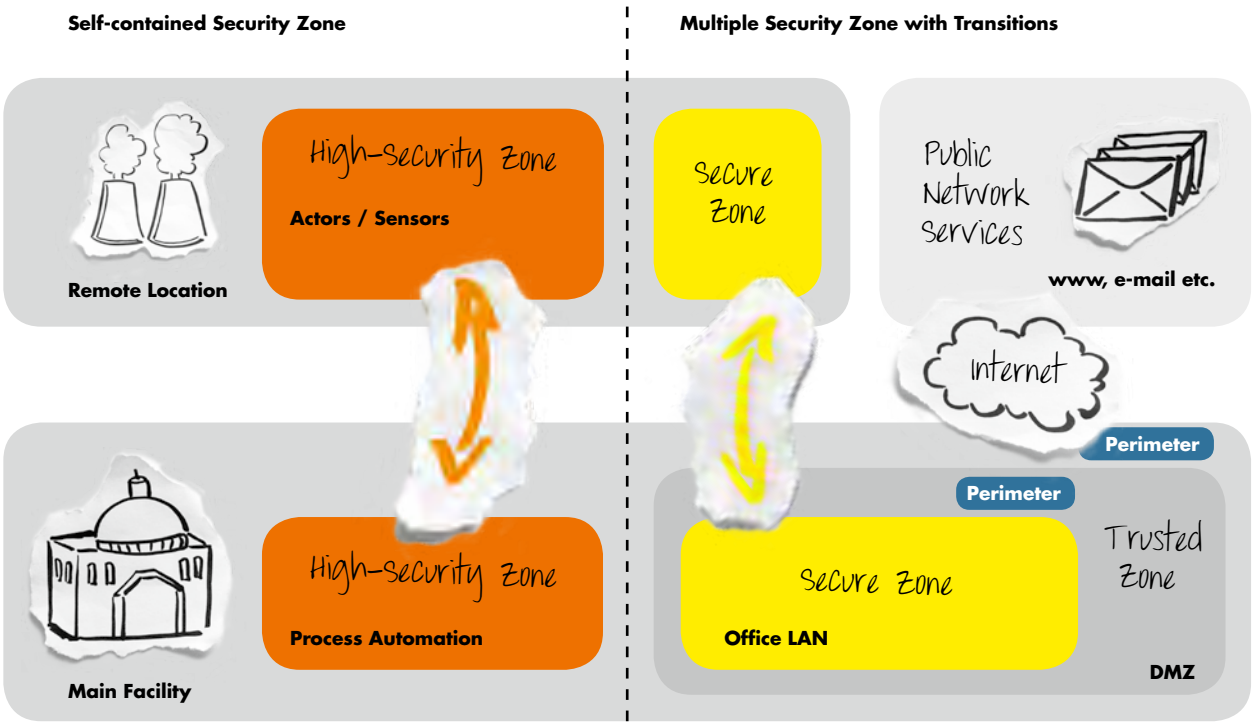
A Copernican revolution

One could almost talk about a Copernican revolution in ICT philosophy. For a long time, the top specification was to achieve as efficient and flexible a flow of data as possible in ICT projects. Today the approach is just the opposite, at least in cases where failures are absolutely intolerable: What specific degree of protection is needed for the data and information used and how can they be kept available, processed, transferred and saved "in a controlled manner" that satisfies these security requirements.

Nicolaus Copernicus was the first to prove that the earth was not in the centre of the solar system but rather vice versa that the earth (and planets) revolved around the sun.



Security Zones and Zone Transitions



Even if two or more locations are linked by means of ICT, the strict separation of the security zones must be maintained. The high-security zone is implemented as completely self-contained. Any data transferred between the locations undergoes high-security encryption. The interzonal transitions (perimeters) between the secure zone and the trusted zone are heavily protected. The public zone accessible to public network traffic is the only zone with direct access to the Internet and other public networks.