Cybersecurity

The internal encoding or deciphering of sensitive data.

With the distribution of the modern computer technique in the seventies a whole number of questions of the protection of the stored information which one could solve with the classic means of the protection of the secrets, no longer effective arose.

So it has lasted for about 35 years until the findings have formed move of the areas of science, research and economy to the protection of stored information.

A short time, only 35 years, and then 30% such a safety solution do not have yet. We generously know nothing about the security systems this one come to the application. But since these systems shall cost nothing if possible a weird safety angedichtet gets that one of ae bent and this. Already the old Privy Councillor Goethe wrote "to literature and truth" how he explicitly did not mention that one of ae.

One also can use him for this purpose, but one will sees reaching very fast the borders. But if one uses him, if one should remember **the** mortal sins of the **cryptology.** A number of known applications is not worth her money because. AES 256 does not lie this. That one of ae used correctly he also solves some problems quite successfully, he is and can not be universal solution according to many users also. It is only a Encoding standards,

The difficulties of the protection of classified programmes were one of the questions then in the computers. The solutions found in this train of the development led to the uncovering of new weak points in the safety philosophy again and again. Tearing or from the view of the modern "patch technology" which after that find of holes simply patches stuck gets, was not possible in this sensitive area this? Even if all problems could not be solved. But these solutions led to a higher standard of the danger defence as a whole.

Become two equipment from this for the representation of a practical solution technology - Fundus KG 200 and KG 201 used. The equipment demonstrates the practical putting into action. You are only regarded as an example. For the algorithms used in this example the respectively current information of the NIST/USA has to be taken into account.

So the used algorithm represents only a manner or function.

4-0-1

They in a way led to a delay of these effective solutions. Detours in the context of which new solution horizons arose had to be gone often.
The solutions to these difficulties were different according to the respective starting-points.

In the course of this development a row became of solution trials develops into independent methods.

So the methods to the protection of the programmes (software) from manipulations or other damages.

One can summarize these under the idea of the hardened software. The programme (software) is available in encoded or encoded form. For the processing in the processor this is decoded or decoded correspondingly. Changes at these programmes carried out lead to a breaking off of the processing.

At another solution this one was " disposable tables gone back on the knowledge. The principles of the deciphering or encoding as a basis were used. With this difference, the secret texts were not transferred but saved on a magnetic data carrier only.

There are two solution trials for this solution variant.

1 The ready information file is encoded after conclusion of the Bearbeitsprozesses or encodes on the magnetic data carrier stored.

2 The Records of the files are encoded and encoded in the regular process. A permanent communication is carried out with the storage medium.

The proposal for solution 1 the - external one solution-

The simple solution (1) has gained acceptance in the weekday.

The "internal deciphering or encoding of information" was also included. This apparently simple formulation proved to be a tough nut since a 1 to 1 take-over of the classic principles of the encoding or deciphering was not possible completely ..

The faults (mortal sins of the cryptology) had to be avoided at the same time, too.

The application of these systems in the computers also provides a number of additional boundary conditions. The question of the irradiation was there/electromagnetic issue or Tempest only a section.

Before you go into this following into the individual systems. Two typical representatives of these information security systems shall be introduced and explained more precisely in the respective sections to them.

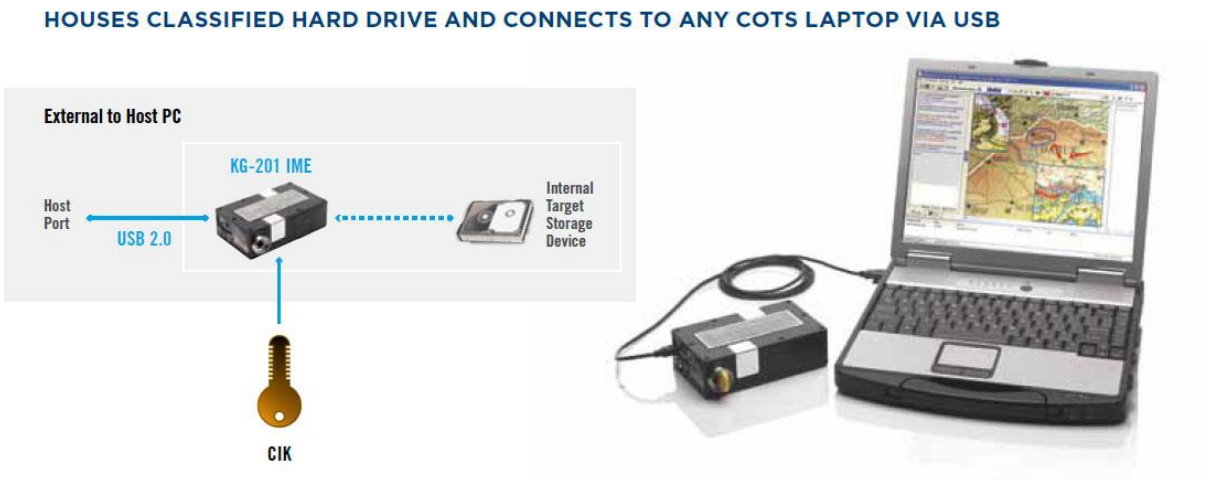
4-0-2

It bargains for the Geräte KG 200 and KG 201 from the USA which have been used also in the defense forces there.

You find the details under Adresse KG 200 or KG 201 and they can look up further information on the side technology ct +VG to 1989.

The following illustration shows the encoding encoding unity between the cybernetic unity and the external data carrier the classification.

Insertion of the illustration of the KG 201



As an algorithm finds the AES 256 use. The passage instalment the encoding encoding - unity 480 Mbps.

This method safeguards the data on an external data carrier. Also at a loss of these data carriers there is generally no danger for the protected information. This data carrier does not need to be now transferred with a special courier service.

They analyse this use of safeguarding systems on her further risks!

You take the present cybernetic, and the way of the successful attacks as a basis

What do these take a look at risks into?

Analyse this application also from the aspect of the effect mechanisms of the modern cybernetic weapons of Stuxnet about DuQu up to Flemish man and his derivations.

Further notes find her left under "cybernetic weapons"

The considerations shall be ended to this simple system in this place.

The proposal for solution 2 the - internal one solution-

A method reminds this of the classic methods of the encoding or deciphering of the ancient times contained this solution.
The processing of the information keeping closed secretly is carried out almost without a human influencing. This process is run through a cybernetic system.

A different one is not called what the protection of the information is a "cybernetic process" and, if they "have not this recognized correctly", leads him into the nirvana. Nothing else is called what, information irrevocably lost (mutilated Chiffrate), a holey security system, therefore one all around safeguards solution for the destruction of information as well as preferential treatment of betrayal of information keeping closed secretly.

They should think also to this if they let themselves in for the following adventure.

Before they want to deal with the question of the "internal deciphering or encoding", they answer the question? What shall be protected?

The deciphering or the encoding serves only the protection, the information processed with these methods. The C-V method does not have influence on possible deletions or by over-spellings (Wiper or Shamoon) . then such attack means be aimed at the destruction of her information by over-spellings of the hard disk (memory) of the computer.

Because the C-V unity receives such an order, these areas of the hard disk are also overwritten or deleted so. This one is only the difference, the over-spelling is carried out with encoded or encoded "information". Compared with the conventional method there is therefore no difference.

The same is the result, with "an internal deciphering or encoding". You have the damage.

The reason for it is not the applied encoding or encoding methods but in the "faulty control" of the internal unity to save her information. The encoding or encoding unity cannot recognize what permitted and what are not. This is not her task.

They must organize this.

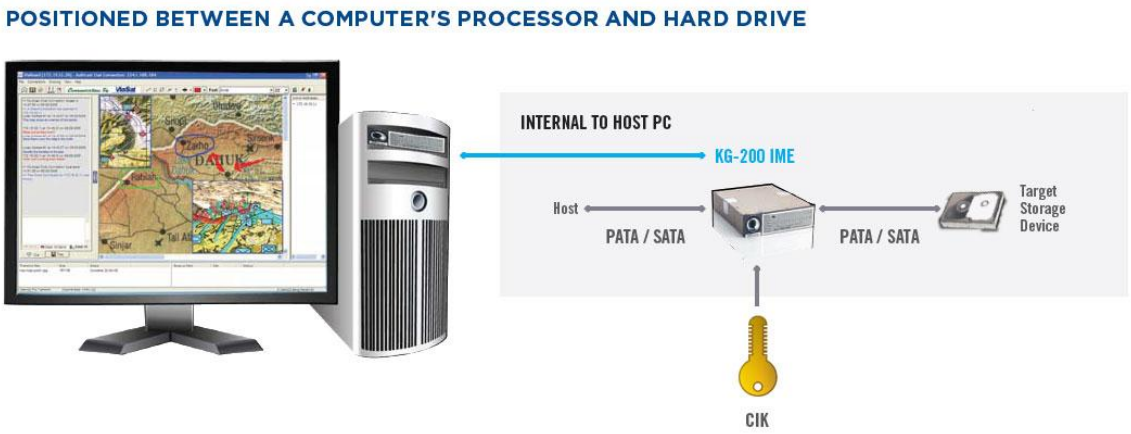
You must create the protection which is required, so that such "harming programmes" or elements reach her hard disk.

A lot of fun with the solution!

4-0-4

We come back, again on the older examples back and look at the KG 200 in the job profile in this place. Illustration KG

200



On the illustration a computer this one is undone at the respective interfaces between the processor and the hard disk see you. This one became encoding or encoding unity into this interface, inserted in this case kg 200.

This unity which functions executes everything, is secret for understandable reasons. Only the used algorithm AES 256 was named. They can do various information about that one of ae this in this forum receivedly, so further explanations are not required in this place.

We look at the internal deciphering in the following a little more nearly.

An illustration which shall explain this more precisely but to this.

You see, it is a relatively simple solution. But only on the first look. Like one says the devil is in the detail because.

These are hidden in the so-called tax module. You must carry out the control of the processes of the deciphering or encoding/deciphering. This module decides whether the following deciphering be fulfilled according to the demanded parameters.

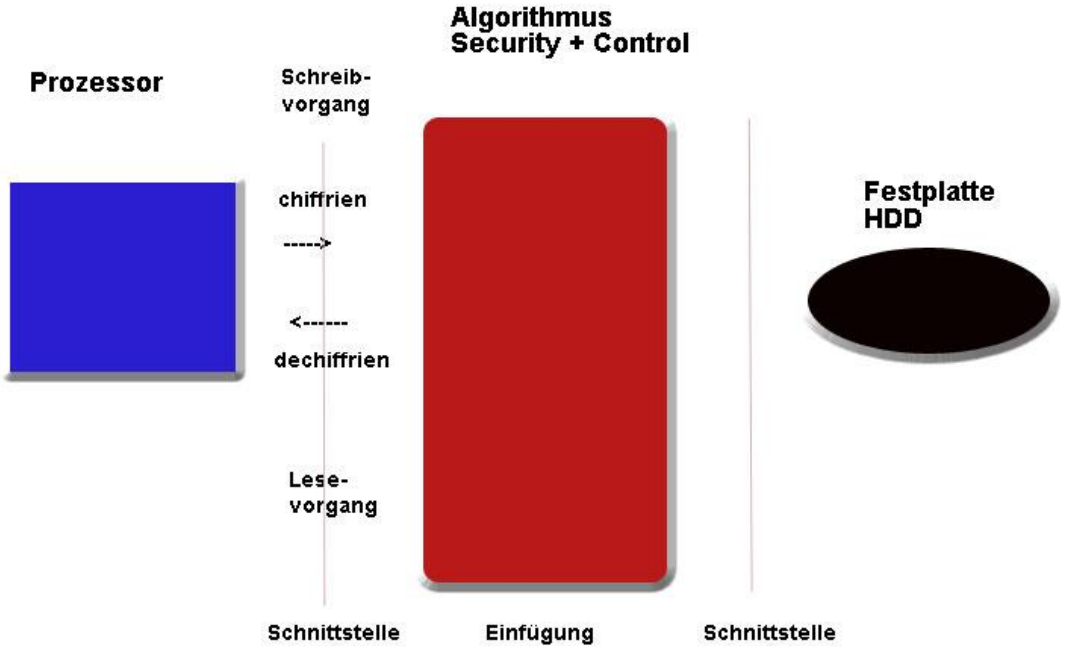
4-05

On the meaning of this module they will be pushed directly if these want to solve difficulties.

It is one of the tasks of the mode to let only the information about the encoding encoding unity which is authorized correspondingly. This shall be excluded, with that harming programmes reach the hard disk.

Therefore you shall not go more nearly into this area.

The information then is encode/will submit encoding module of this area to this.



This module runs the AES 256 algorithm through the transformation under use through.

Which boundary conditions must be complied with.

1 The number of information per sector
2 The key construction for the automatic mode
3 There are which cryptic logical requirements for the information data.

4-0-6

1 The information is available at the interfaces to ATA in serial (S) or parallel (P) form. The information to be saved on the following data carrier (hard disk) has a length of 512 bytes. The AES 256 has a length of 32 bytes or 256 bits. Being sector 16 encoding processes needed for the encoding of one with that. 512 bytes are then encoded with that. This process must be carried out with a speed of 800 Mbitps. These requirements are by the AES 256 fulfils. The complete process of the encoding therefore lasts for 5.12 microseconds (5,12!) 0-6 seconds.

2 The key construction is automated at this process. The made keys reject an internal dependence of the number of the sector and key made for this. Because the combination of the sec fool number makes the production of a key possible for the sector with a key sequence which is entered externally. A

deciphering or encoding of the information makes it possible dependence of the key of the number of the sector.
The key, as follows formed could be with that:

Variable value = key (x) number of the sector (x) + x for the sector (.)

If they have knowledge from the deciphering with disposable keys, the period number corresponds to the sec fool number so.
The analogy is, without the key period they can not decode this period of the secret text.

Boundary conditions:
From the sec fool number you cannot close on the key of the necessary sector with the condition.

There is no dependence between number of the sector (x) and the key (x) either.

There she in this but with a variety of keys (y) auc H may be able infer from the variety of the sec fool number on the construction of keys it not only with a key (x).

3 The algorithm AES 256 is used in this concrete case. The AES 256 sets voraus. a careful planning the use.

They also comply with the boundary conditions of the use and the required cryptic logical strength.
The information to be encoded has a length of up to 512 bytes.
The AES 256 has a length of 32 bytes or 256 bits the key.
Which method they use depending on be able to 32 bytes unite her - use keys and 512 bytes encodes with that. However, you also can use 16 keys with a length of 32 bytes.

In the the latter case they obtain a very high cryptic logical strength.

Which method is required, gets only and alone by the requirements on the protection of the information.
4-ß 7

The concrete application is . - , however, are the solutions in a very interesting way and relatively renounced in this place to realize low effort.

Be able to do her for further questions for us this by mail to the web address;

webmaster@gocs.de

Author: Old Gocs

Berlin, November 2012