CyberContract

PREVENTION

CyberContract offers companies access to a unique set of specialised services with local professionals. Services of proven quality... rapid and centrally accessible. This way, we assist you very specifically in elaborating a prevention plan concerning cyber incidents. After all, prevention is always the first step!

We have strong partners for the following preventive services, among others:

PEOPLE AWARENESS

INFRASTRUCTURE AUDIT

NETWORK AUDIT

SECURE

SOFTWARE LEGAL

Kempenlaan 29
2300 Turnhout

Doopput 14
2550 Kontich

www.cybercontract.eu
info@cybercontract.eu

Independent intermediary FSMA 113529A - RPR 0557.948.651 - BE02 0017 4242 4740

PEOPLE AWARENESS

Are your people trained on security awareness?

Every employee should be aware that he or she could be contacted at any moment by someone to extract information. Someone who suddenly calls with a few seemingly innocent requests for more information, an odd-job man suddenly walking around, and even the correct use of passwords are issues all staff should be trained on.

How to increase awareness?

There are unfortunately not golden rules for increasing awareness, since this is always company-specific and has to "fit in" with the company's culture. This is sometimes possible through one-to-many training sessions or is sometimes possible using computer training, yet there are also possibilities such as a short company film or other creative options. Our consultants have been applying various strategies for years, and can hone these perfectly to your culture.

How can you test it?

Testing is possible in various ways, and the most common tests we assist companies with include the following:

- Sending phishing emails of various levels, starting from blatant phishing (such as the King of Namibia) to highly focused emails, whereby the employee is addressed in correct use of language by his/her first name in a credible scenario.
- USB drop-offs whereby reports are made to present what percentage of USB sticks were connected with a PC, what percent of people opened files from the stick, etc.
- Social engineering whereby specific goals are approached to verify whether or not company policies on releasing specific information is being followed. This can occur both by telephone and in person.

SECURE INFRASTRUCTURE

Data loss prevention: control over your data

What might the recipient do with your email when he/she receives it? What if your employee places all the data on a USM stick and resells this? These are questions that keep every business leader awake, which is why every company should have elaborated data-loss prevention techniques whereby, for instance, it is no longer possible to copy data or print or forward emails. There are various solutions for this, and we can assist in making the right choice and deployment.

Internal penetration test: the insider hacker

What if someone just wanders in and connects their laptop to the network – can they inflict damage? Can they commit data theft? Or could disgruntled employees stop servers or spread viruses? You should know and not fear the answer to this, and it is thus extremely important to have a consultant with a hacker mentality perform a regular check, who can explain what actions should be taken to take security to a high level.

Active Directory security health check

The Active Directory is often the database in which all users are defined, yet is unfortunately also often not under control due to years of migrations form old to new versions, or due to poor everyday monitoring. It is soon forgotten that employees leave service and retain all rights to log in remotely, or there are often a lot more administrator users than supposed. It is important to perform a test so as to take focused actions based on the outcome, to protect the environment's heart from misuse.

SECURE INFRASTRUCTURE

Virus outbreak

Even if anti-virus is installed on every device, a virus regularly slips through the mesh of the net, and then manage to seriously escalate. Consider the recent outbreaks of ransomware whereby data was made unreadable and a hacker asked for money to reset everything. But does paying ransom stop after once? Following a virus outbreak, it is extremely important to be able to call on the right people who can keep cool-headed together with you and swiftly undertake the right decisions.

Certificates: how to use them correctly

Certificates are used for numerous applications: for securing websites (https://connections) or protecting sensitive data internally. Unfortunately, the plan is frequently no more than a few thoughtless clicks, meaning problems are later encountered. A considered design is extremely important, and experience is the first requirement in this regard.

NETWORK REVIEW

Checking the design of your network

When designing a new network or redefining an existing one, it is important that this can be viewed together with experts so as to ensure all known pitfalls are avoided. After all, once a new network has been put into place, it is much more difficult to then introduce drastic changes.

Penetration testing from the outside: who can get in?

Every minute an external IP address is attacked over the internet by one of the countless automatic scanners that exist, yet in Belgium focused attacks are increasingly occurring. Hackers often try to penetrate weakly protected firewalls in order to thus proceed to the inside of the company. A external check is often more limited due to the low number of open ports available, yet has to be checked all the more strictly so as to minimise the risk of a successful attack.

Red team exercises: test my security

More and more clients want to know what's possible in a realistic attack scenario: Is it possible our customer information can be stolen? They also want to gauge this by initiating a test, whereby little to no information is released and the assignment consists in launching an attack without many people being informed of this internally within the business. This way it can be examined not only how difficult it is to get inside, but responses can be also be tested if internal IT sees that certain issues are occurring and they are slowly losing control.

SECURE SOFTWARE

Already start during a project, not after it

You develop secure software from the very start. Since security in software is something extremely specific, you should not do this yourself but involve an expert promptly. This expert does not even need to be constantly involved in the project, but can for instance get together with the project's stakeholders once a week to deal with specific questions regarding security. This expert can guide you in taking the right decisions, and can test penetration in the most appropriate manner for planning the software, so that work is performed with a view to quality and cost efficiency.

Developers? Get training!

While the majority of developers are familiar with a number of security risks, they unfortunately so rarely encounter them that they're often forgotten in practice. It is extremely important that developers take training whereby they themselves get the opportunity to attack a number of example applications or their own applications. By doing it themselves, they realise not only that it is not always difficult for hackers, but they are become more conscious of the risk, meaning in the future they will be much more aware and enlist help promptly.

Penetration testing op applications

In these times it is no longer responsible to continue publishing applications on the internal or external network without first subjecting them to a penetration test. The importance of this should not be underestimated, since hackers will always damage a company publicly by making it known, for instance, that a database was stolen, or by them extorting or asking for money not to publish data acquired. It must be verified annually whether any new exploits are known that could be misused for attacking the application, and whether any code was added containing errors whereby the application runs an increased risk.