Protect the castles!

Cyber risks explained for everyone

cysmo® POWERED BY ppi

PPI AG supports insurance companies with the cyber risk rating tool cysmo® in the real-time assessment of companies.

Fully automated and at the touch of a button, cysmo® analyses the success probability of potential and real existing cyber attacks.

cysmo.de/en/business-suite

cysmo® – Protect the castles!

For a better understanding of the issues in the cyber environment, the cysmo® team metaphorically illustrates different cyber scenarios with this series of stories called "Protect the castles".
The castle always symbolises a company – the people involved are the managers or employees of this company.

I. #DDoS attacks – **Chaos at the gate!**

II. #Hacks – **Attack on the wall!**

III. #DNS attack – **Where's the mail?!**

IV. #Spoofing – **The false judge**

V. #Blacklist – **Even a king cannot know everything**

VI. #Data theft – **New danger from the darknet**

Here we go ...

#DDoS attacks – Chaos at the gate!

Merchants enter and leave your castle every day. The guard checks all unknown faces at the entrance, protecting your castle from spies and saboteurs. But your rival doesn't leave it at a few spies: He launches a DDoS attack and sends a multitude of spies to your castle.

He also deceives uninvolved messengers who don't actually do business with your castle and lures them to your gate. At some point, their guard can no longer handle this onslaught: the queues at the gate become so long that not everyone can pass. The operation of the castle comes to a standstill.

DDoS attacks: A large number of bots (or botnets) overload a system (such as an e-mail server) so that it is no longer accessible for normal requests.

#Hacks – Attack on the wall!

In our castle world, a hack would amount to a real attack with the aim of secretly plundering the castle. The attacker first scouts the castle and analyses weak points and possible attack scenarios.

He has two options here:

- **Passive** (reconnaissance from a distance)
- **Active** (testing the defence with the risk of unmasking)

Hacks: In the field of computer security, a system is considered hacked if a security mechanism has been broken or bypassed, the hack being the action by which the goal is achieved.

#Hacks – Attack on the wall!

The attack is then launched. The attacker attempts to penetrate the castle via the previously identified vulnerabilities (e.g. open ports).

In addition to extortion by encrypting data (ransomware), such as for WannaCry incidents, there are various other attack possibilities.

Data theft or using the infrastructure for botnet attacks are just two examples. This makes it difficult to analyse the damage.

#DNS attack – Where's the mail?!

The few signposts to your castle have been removed, turned over or blocked.
Your castle is accessible, but without the precise knowledge of its location,
it is still impossible to reach it.

Now that you've identified the problem, you can fix it quickly.
But the messenger you were expecting is already on his way back.

DNS attacks: The DNS amplification attack is a denial-of-service attack that uses the domain name system to direct extremely large data streams to the victim's Internet connection.

#Spoofing – The false judge

The perpetrator of past attacks has been caught.
The king (lord of the castle) is waiting for the arrival of the judge.

When he finally shows up, however, his verdict is sobering:
the prisoner is released immediately and rides off with the judge.

Spoofing: Spoofing (i.e. manipulation, concealment or pretence) is the IT term for various deception methods in computer networks to conceal one's own identity.

#Spoofing – The false judge

A short time later a second judge comes to your castle:
It turns out the first was an impostor, an accomplice of your rival who was only posing as a judge.

The seal on the judge's letter was fake; you've been tricked.

#Blacklist – Even a king cannot know everything

The king wants to collect as much information about the merchants in his castle as possible. But all of a sudden, all of this data – where merchants live, what they trade, how much money they get for a delivery, and much more – is on lists and openly lying around on the town square.

An unknown person was able to exploit this. Using the information, he impersonated the merchants and sent your customers bad fruit by the dozen.

Blacklists: A blacklist contains networks that have attracted attention due to dubious traffic.

#Blacklist – Even a king cannot know everything

The customers have reported the deliveries and now your merchants have been blacklisted; no one wants to buy anything from you anymore.

If the king had not wanted to know everything and had not stored all the information, the data of the merchants would not have been circulated.

#Data theft – New danger from the darknet

And it gets worse! One of your merchants was robbed due to an unlocked door and his list of symbols and passwords was stolen during the robbery.

The thief (hacker) now drives into a forest (darknet) and brags about his stolen goods to other thieves. He offers the lists to the other thieves to buy.

Darknet: In computer science the darknet ("dark network") describes a peer-to-peer overlay network whose participants establish the connections with each other manually.

#Contact – The right contact person to ensure that you always have an eye on the security of your castle ...

Jonas Schwade

Phone +49 211 975525035
Mobile +49 151 26737115

Jonas.Schwade@ppi.de

PPI AG
Peter-Müller-Str. 10
40468 Düsseldorf
Germany

Sebastian Scholz

Phone +49 40 2274331725
Mobile +49 151 62836107

Sebastian.Scholz@ppi.de

PPI AG
Moorfuhrtweg 13
22301 Hamburg
Germany

Jonas Schwade is a senior consultant at PPI AG and product owner of the cysmo® Business Suite. His focus is on cyber security, sales processes and agile IT development processes.

Sebastian Scholz is a partner at PPI AG and is responsible for the cyber business segment. With 10 years of consulting experience, he specializes in insurance processes, cyber security, underwriting, IT implementation and analytics.

www.cysmo.de/en

cysmo®
POWERED BY ppi