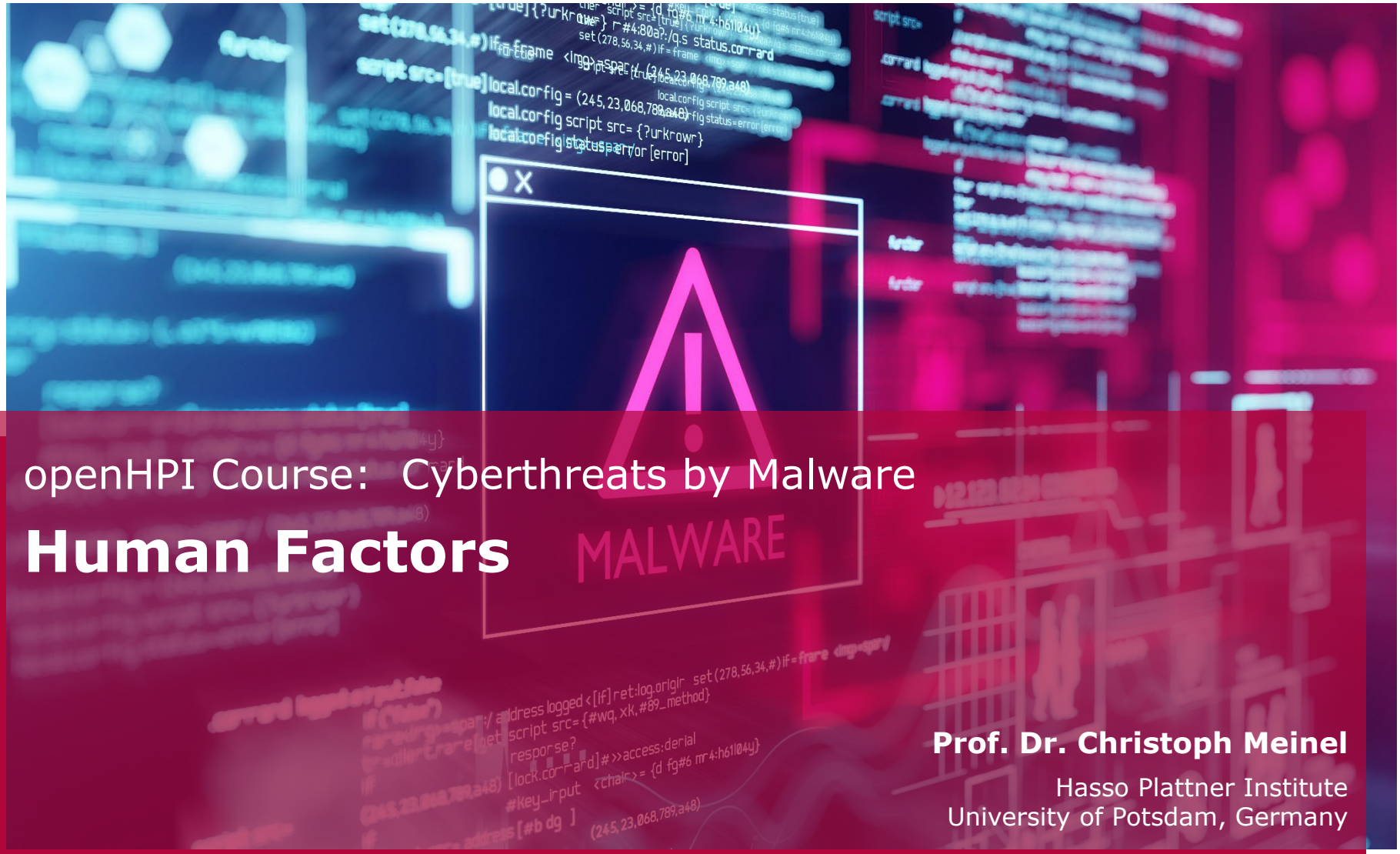

openHPI Course: Cyberthreats by Malware

Human Factors

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Human as a Security Risk

Human factor stands for all human aspects that could create security risk in the system

Two categories of human factor can be distinguished:

- **Active**: Risk is caused by unknowingly or knowingly doing certain activity
- **Passive**: Risk is caused by not doing certain activity that should have been done

Social Engineering / Social Hacking Attacks

Attackers try to **impersonate** other people or systems (website or application) to **trick users** to **share secret personal information**

Example:

- User gets a phone call from unknown number
- Attacker tells that he is an employee from the user's bank and needs his help to check for **potentially fraudulent bank transfers**
  - creates a **stress-situation for the user**
- Attacker then asks the user to tell his banking private details to "verify" the fake transfers
- Attacker can then use the user's data to **maliciously authenticate himself with the bank**

Active Human Factors: **Email Phishing Attack**

Attackers often try to send emails with malicious attachments (including malware) to users

- Attachments of emails can often **contain malware**

→ **It is up to the user to be aware of this threat!**

- If an email is **not expected / from a unknown person**, do not open the attachments!
- If an email appears to be from colleagues but **sounds suspicious**, ask the colleagues through a different channel (e.g., call, talk, SMS, …) if the mail comes from them

Active Human Factors: **Spear Phishing Attack** (1/2)

Traditional widespread phishing is no longer effective for obtaining the victim's personal or confidential information

Attackers therefore turn to **personalized phishing** or **spear phishing**

- Attackers **collect highly detailed information** about their victims to later use is for gaining their trust
  - collect the references of a person (e.g. friend, family member, colleague) that the victim knows and trusts from social media or web presence
  - victim believes that the email comes from the trusted person because the message contains information only that person knows

Active Human Factors: **Spear Phishing Attack** (2/2)

- Spear-phishing attacks have a much higher success probability but require more works for the attacker
- Personalized phishing is therefore very dangerous and will be applied to target
  - **important people**, e.g. CEOs, politicians, high-ranking officials, celebrities, ...
  - **sensitive sectors**, e.g. military, business, politics, financial, ...
- The attacks could be launched by states, activists, hackers, organized crime, ...

Note: Many other attacks on the Internet are based on previous personalized phishing attacks

Passive Human Factors

Even when a company is providing good security guidelines, there might be **employees who simply do not care nor follow the guidelines**

- They **fail to adhere to the guidelines** / standards
- Could cause security problems because they are **not doing what they are supposed to** do
- A solution for this problem is dedicated information sessions or workshops
  - **sensibilization** of the employees for the topic
  - depiction of **results of lack of caution**

The weakest link in the security chain is often the human being!