



openHPI – Internet Security Malware: Protective Measures

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

Regular Backup (1/2)

Malware attacks on the Internet often cause **loss of** or **damage to data**

- If data is lost due to viruses, ransomware or operating system damage, data can be restored from previously created backup copies - "**backups**"
- Important and personal data must therefore be secured on a regular basis
- Systems offer automatic data backup in predefined time intervals
- Save backups to external media
- Keep external media physically separate from the computer
 - If an attacker completely takes over your computer, he/she has no way to access data backup

Regular Backup (2/2)

Malware attacks on the Internet often cause **loss of** or **damage to data**

Data can also be stored **online** (e.g. in the cloud)

- This requires secure control of access to the personal data
- Encryption of backups is recommended
- Do not keep a permanent connection to online backup media as local changes are directly transferred to the on-line store
- Saving different versions allows you to undo specific changes if necessary

Program Updates (1/2)

Program updates are used to resolve known vulnerabilities in software and thereby eliminate security risks

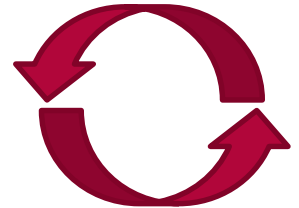
- Use of (older, not updated) software versions poses a security risk because of the increased risk of abuse of revealed vulnerabilities

Always perform updates as they become available:

- Vendors do not find all breaches during the test phase. Many vulnerabilities in programs are often discovered only after publication, e.g. by
 - Analysis by external experts, known attacks, ...
- Known security breaches can usually be closed by small update packages

Program Updates (2/2)

- Modern programs often automatically inform of existing updates
- In addition, there are applications that automatically look for updates for the installed software
- Some antivirus programs check whether the installed software is up to date



But with all updates, the following applies:

- It is essential to verify the trustworthiness of the source and the update
- Otherwise, updates themselves can become the source of new attacks and enable the installation of malicious software
- ...

Virus Scanners - Antivirus Software (1/3)

Virus scanners and **antivirus software** provide methods for detecting malware

- Can also detect worms, trojans, spyware and other malicious software
 - Therefore, these products can also be better known as **antimalware software**
- Some of these products also monitor Internet connections and warn against unsafe websites
- Now a **compulsory element** of Internet-connected systems and integrated into them

Virus Scanners - Antivirus Software (2/3)

Antimalware software is based on two different detection methods:

■ **Signatures**

- Signatures are obtained through analysis of malware and "describe" distinctive characteristics of the malware
- Files are checked for these characteristics and classified accordingly

■ **Anomalies**

- The normal or "benign" state of the system is detected and then constantly compared with the current state
- A warning is generated if there is a strong deviation from the current state
- Enables detection of unknown malware – however, anomaly-based methods are often less accurate

Virus Scanners - Antivirus Software (3/3)

- Antimalware software must always be kept up-to-date
 - Continuously updated virus definitions and signatures also enable the detection of new viruses and malware
- Ideally, all data sources must be searched for viruses
 - Hard disks, removable media (CD, USB sticks, ...), network connections, ...
- Most virus scanner automatically block, prevent installation and remove malware, but if viruses are found more frequently a manual investigation of the cause can help
- Infected systems tend to be slower, unsafe, or to drop out completely. Therefore, the virus / malware warnings should be taken seriously and the problem should be resolved as quickly as possible

Firewalls (1/2)

Firewalls monitor all incoming and outgoing network connections and the data traffic passing through them

- Can prevent unauthorized connection attempts
- Provide additional protection against attacks, such as by backdoors or botnets
 - Each attack will create a connection to/from the attacker that has not been approved by the user. This connection must be prevented or an alarm should be triggered
- A local firewall acts only on the system on which it is installed
- A network firewall checks all network traffic and is usually installed on connection nodes between a local network and the Internet

Firewalls (2/2)

The function of a firewall is controlled by so-called rules

- Rules define which connections are allowed and which are not
- Rules can be formulated specifically for individual applications, protocols, ports, and addresses, and define exactly what is permitted and what is not
- If a rule applies to a network package, various actions can be performed
 - Data package can be modified or completely blocked
 - Warnings can be displayed
 - ...
- **Windows Firewall** is active by default
- GNU/Linux also provides a firewall with **iptables**

Healthy Mistrust (1/2)

Healthy mistrust is the most effective protection against malware infections

- The best warning and protection mechanisms are invalid if the user still opens untrustworthy content
- When installing new software, always check manufacturer and origin
- Verify the signature of the software / updates to be installed (can be done automatically)
- In the case of a warning, manual verification is required
- Only install software that is really needed
 - Unnecessary applications, add-ons, additional features, optional plugins provide unnecessary attack vectors for attackers

Healthy Mistrust (2/2)

- Switch off active content (Flash, Java, Active X) in the web browser, since these offer various attack and break-in options
- Use "cookies" only for trusted pages
- Only open e-mail attachments when
 - sender is known and text can be assigned to the sender
 - an e-mail with attachment was expected
- Keep calm when faced with online warnings and calls for payment of fines
- Check installed software and remove any unused, unnecessary programs