Virtual Patching

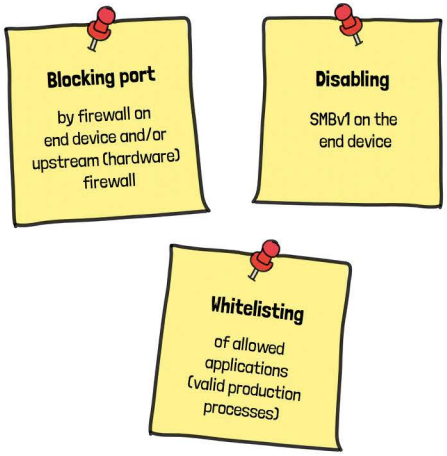
A **virtual patch** does not repair the actual broken application but establishes a security mechanism that is intended to prevent the exploitation of a vulnerability.

In contrast, **„classic" patches** correct errors in programs and close security holes.

In short: **A virtual patch does not fix the actual cause, but only the symptoms.**

Implementation

Regarding the example: "WannaCry" ransomware on Windows (XP) systems in production by blocking SMBv1 traffic



Advantages and disadvantages

of virtual patching

Advantages:

- **Speed**
  Immediate response to security risk possible
- **Unhindered rollout**
  Installation usually occurs without disrupting ongoing operations e.g. system reboot

Disadvantages:

- **No sustainable protection of the systems**
  Only useful as a transitional measure
- **Restrictions in the range of functions**
  Access to functions or endpoints may have to be blocked

Virtual vs. classic patching?

Both virtual and classic patching are effective security measures that can be used in their respective use cases.

General rules:

Virtual patching is not a substitute for the actual fixing of the vulnerabilities via classic patches

Choose your patch type wisely and consider consulting from experts!