Classification of Microsoft updates
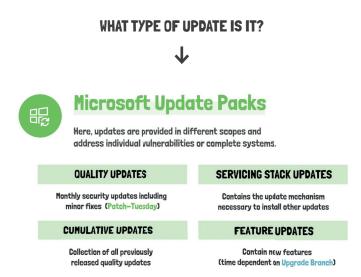
WHAT IS THE SECURITY RISK?

↓

Security Update Severity Ratings

In order, to assess the need for a patch, four rating categories with corresponding recommendations for action were created.

1	Critical	Apply immediately!
2	Important	Apply as early as possible!
3	Moderate	Apply security updates!
4	Low	Evaluate whether it makes sense to apply the security update!

WHAT TYPE OF UPDATE IS IT?

↓

Microsoft Update Packs

Here, updates are provided in different scopes and address individual vulnerabilities or complete systems.

QUALITY UPDATES

Monthly security updates including minor fixes (Patch-Tuesday)

SERVICING STACK UPDATES

Contains the update mechanism necessary to install other updates

CUMULATIVE UPDATES

Collection of all previously released quality updates

FEATURE UPDATES

Contain new features (time dependent on Upgrade Branch)

HOW LONG WILL THE UPDATE BE DEPLOYED?

↓

Microsoft Upgrade Branches

An update branch defines how long an update can be delayed. Since 2018, the following two branches are in use.

LONG-TERM SERVICING CHANNEL (LTSC)

- For enterprise users
- Support for 5-6 years
- Formerly LTSB

SEMI-ANNUAL CHANNEL (SAC)

- For SOHO users
- Support for 18 months

Whether and when updates and patches should be installed depends, among other things, on the availability of the environment and criticality of closed vulnerabilities.

Rule of thumb

ENVIRONMENT:				
Critical infrastructure			Evaluation	
Production		Function test		
Office	ASAP			
SEVERITY RATINGS:	1. Critical	2. Important	3. Moderate	4. Low