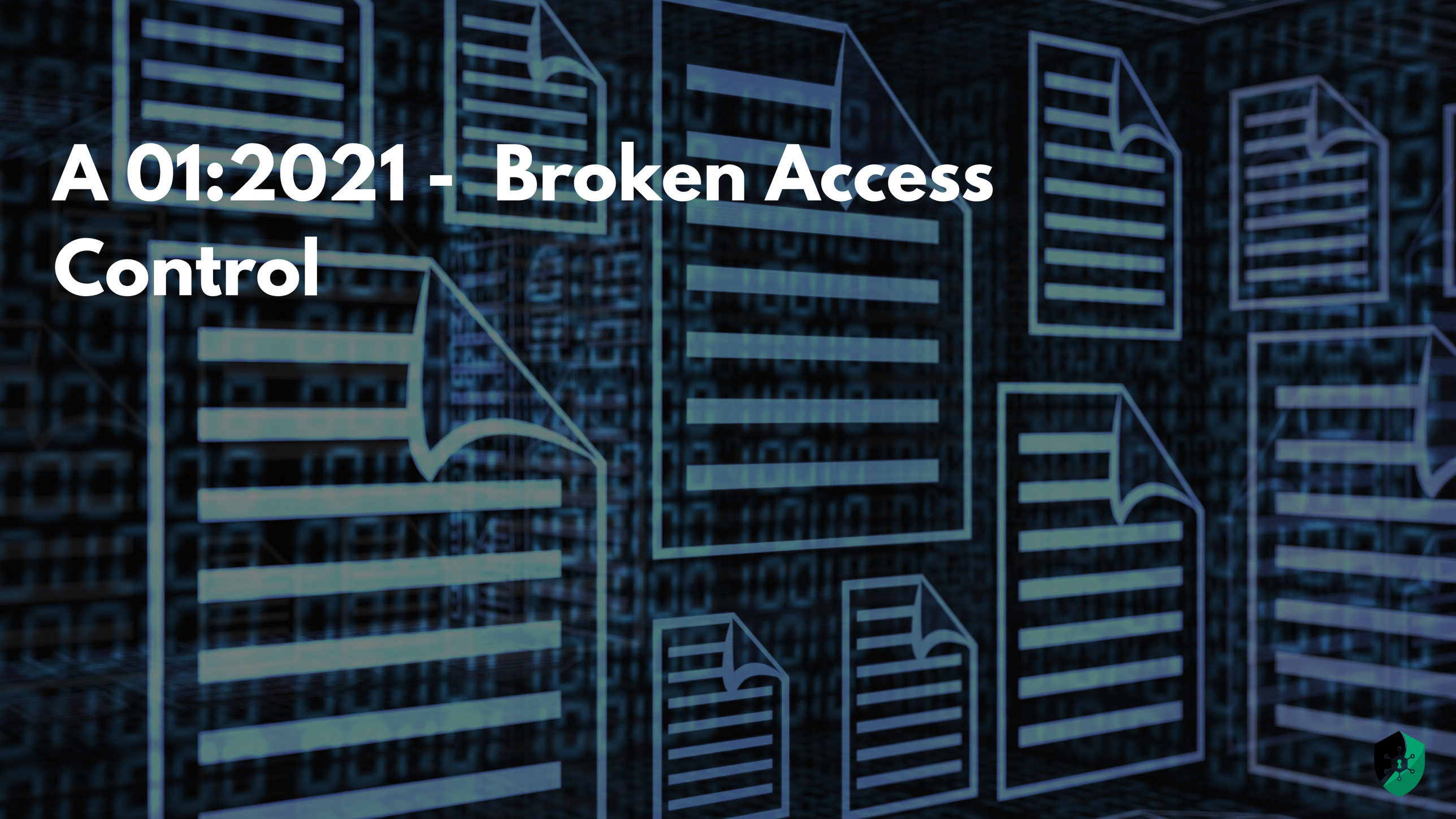
A 01:2021 - Broken Access Control



Access Control

A process for ensuring only authorized users have access to certain types of data

Access Control

Access control enforces policy such that users cannot act outside of their intended permissions.

Broken Access Control

This typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

Broken Access Control

Elevation of privilege. Acting as a user without being logged in or acting as an admin when logged in as a user.

Broken Access Control

Horizontal privilege – the user gets access to different resources other than the one intended for them

Broken Access Control

Can also lead to the unauthorized access of sensitive links and web pages/files on a website due to the fallacy of ***security through obscurity*** (the belief that anything that exists on a website that isn't linked or indexed cannot be found)