7 Deadly Sins

of Security Policy Change Management

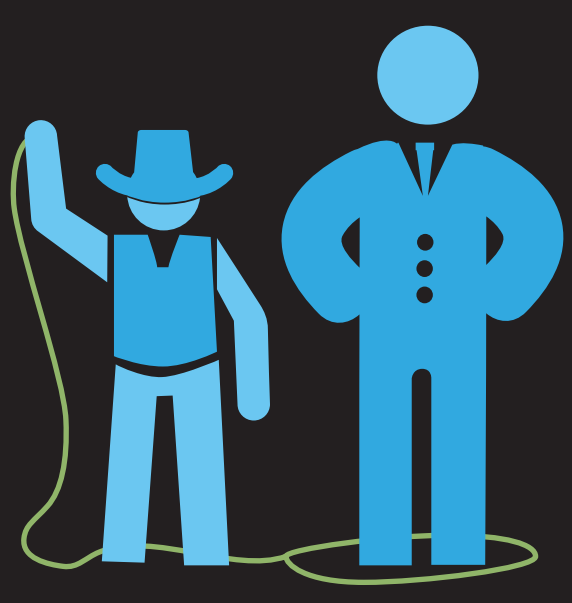
1 Focusing on the "plumbing" instead of on the business applications

2 Not removing firewall rules for decommissioned applications

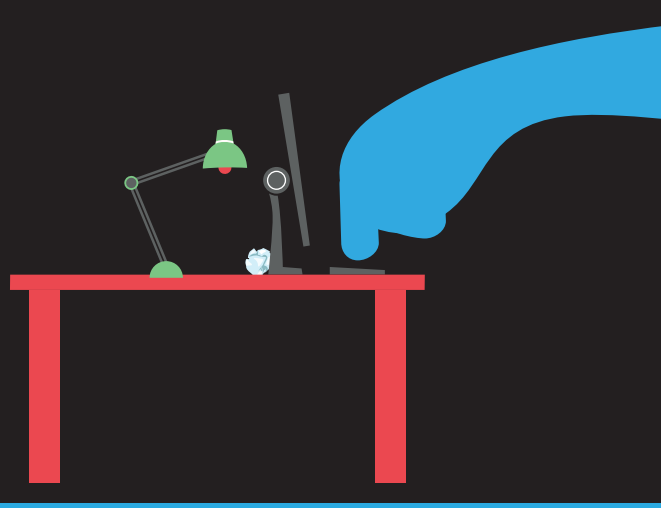
3 Ineffective communication between teams

4 Not documenting enough (or at all!)

5 Not reusing existing firewall rules and objects



6 Not checking if changes are authorized, necessary or documented (no cowboy changes!)



7 Manual "fat finger" input mistakes (port 443 instead of port 433)

Brought to you by:

algosec

www.algosec.com