Details of the VM backup/restore procedure should be in place for commencing patching of servers.

Steps to be taken.  
  
  
  1.  Review available packages to be applied ( **yum check-update**) / (**yum repolist**). This will also check red hat subscription is current (**subscription-manager status**)  
  2.  Review system logs and ensure there are no current issues before proceeding.  
  3.  Confirm with IT staff on the exact time to start patching  
  4.  Request IT to take a VM backup /snapshot or make sure a proper backup or way to roll back is available  
  5.  Patch the system - yum update --security -  this will apply security-related package updates  
  6.  Reboot server to pickup the latest kernel that has been applied ( **shutdown -r** ) to gracefully reboot it, rather than force.  
  7.  Ensure all services (including Database and critical processes) have started after reboot.

From time to time, there will be in Redhat where an RHEL OS version is not supported, and to get security updates will need to update OS.

<https://access.redhat.com/discussions/5509261> Upgrade from RHEL 7.6 to 7.9.

<https://access.redhat.com/solutions/253273> How to register and subscribe a RHEL system to the Red Hat Customer Portal using Red Hat Subscription-Manager?

<https://access.redhat.com/solutions/265523> Enabling or disabling a repository using Red Hat Subscription Management