Notes on security risks priorities 2019

Loris Renggli, 18 Jan. 2019

The Comité de Sécurité Informatique (CSI) in its Jan 10\textsuperscript{th} 2019 meeting has agreed upon the following list of risks which will be addressed with high priority for the coming year.

1) Identification / access
2) Loss or theft of data
3) Users training/awareness; prevention
4) Obsolete OS’s
5) SMB v1
6) Network zoning

Actions to address these risks will have to be defined and progress will be monitored.

Actions for SB

The above list will be communicated to the Comité de Coordination Informatique SB and discussed during the next meeting (Monday 21\textsuperscript{st}). In particular, pro-active actions can be taken without waiting for CSI instructions:

1) Encourage users to change password if older than, say, 1 year. Remind them to keep it secret and never share it with anyone (not even the IT staff, or their boss).
2) Promote usage of personal backup (Druva inSync). Recommend encryption of laptops. Keep track (inventory) of which machines have been encrypted.
3) TBD
4) Non upgradeable machines should be isolated on the network. Windows 7 machines should be upgraded to Windows 10 (availability of all updates – including security ones – for Windows 7 will end in 2020).
5) Make sure all SB servers have SMB v1 disabled. Warn users that SMB v1 will be disabled on central storage (NAS service).
6) Machines in 4) which cannot be upgraded can be moved to an appropriate zone, or, if need be, new zones could be defined. Virtual machines on VPSI’s virtual infrastructure should make use of micro-segmentation (i.e. define with which machines they are allowed to connect).