Versleuteling toepassen op je laptop

HOUD JE GEGEVENS VEILIG BIJ VERLIES MET LUKS

Het verliezen van je geliefde, met zorg uitgekozen, laptop is uitermate vervelend. Gelukkig heb je een back-up gemaakt, maar toch levert het je een ongemakkelijk gevoel op. Je vraagt je af of de privacygevoelige gegevens, die je hebt opgeslagen, wel veilig zijn. › **Paul Reemeijer**

Hardware is vaak wel vervangbaar. De gegevens zijn aanwezig in een van de gemaakte back-ups, maar je wilt niet dat de privacygevoelige gegevens worden misbruikt voor andere doeleinden. Versleuteling is hierbij een uitkomst. Gevoelige gegevens op een versleutelde harde schijf of partitie opslaan zorgt dat de stress voor privacy bij het verliezen van je hardware verminderd.

Onder Mac OS is standaard Filevault te gebruiken en onder Windows is dit Bitlocker. Dit artikel laat je kennis maken met LUKS op Linux.

LUKS gaat op verschillende manieren besproken worden. Als eerste bij de installatie van een Linux-distributie op een schone, nieuwe laptop. Daarna als loop-device binnen je bestaande Linux installatie. Waarom deze optie? Het is namelijk niet mogelijk, zoals bij de andere twee genoemde OS-oplossingen, LUKS te activeren na een installatie zonder gegevensverlies. Als laatste wordt uitgelegd hoe je een USB-drive voorziet van LUKS.

NIEUWE INSTALLATIE

Hieronder een kort, oppervlakkig onderzoek, bij het (op)nieuw installeren van een laptop om te ervaren hoe makkelijk het is om LUKS in te zetten, met behulp van een installatiewizard van een distributie.

Screenshot 1.

De eerste distributie is OpenSUSE Leap 15. De installatiewizard volg ik door de default voorgestelde opties aan te houden. Bij de vraag voor de indeling van de harde schijf niet.

Versleuteling zet je aan onder de optie **Guided Setup**. Verder volg ik de wizard voor de installatie. Na de installatie reboot ik de machine en tot mijn verbazing wordt er een wachtwoord gevraagd nog voordat ik GRUB boot opties te zien krijg, zoals te zien is in **screenshot 1**.

De tweede distributie is Debian, de stabiele versie bij het schrijven is 9.6. Bij deze installatie volg ik tevens de standaard voorgeselecteerde opties van de installatiewizard. Bij het partitioneren van de harde schijf kies ik de enige wizardoptie met versleuteling in zijn omschrijving, "Guided – use entire disk and set up encrypted LVM" (zie **screenshot 2**) en volg ik verder de installatie.

Na de herstart van de machine ontdek ik een klein verschil. Dat verschil is dat ik bij Debian wel eerst GRUB boot opties krijg en daarna pas de vraag om het opgegeven encryptie wachtwoord in te voeren. Als ik kijk naar de partitie-indeling van beide installaties, zie ik dat `/boot` bij Debian op een partitie staat met EXT2 zonder LUKS.

In dit korte en bondige onderzoek is mijn conclusie dat bij beide distributies het niet moeilijk is om LUKS in te schakelen bij de installatie. Bij beide heb ik niets in Expert modus bij SUSE of Manual bij Debian gedaan om LUKS in gebruik te nemen. Versleutelen van de SWAP-partitie is belangrijk voor als je bijvoorbeeld je laptop in hibernation wilt plaatsen. Hibernation zorgt ervoor dat de sleutel voor de in gebruik hebbende versleutelde partities wordt weggeschreven op de SWAP-partitie. Deze waarschuwing en meer achtergrondinformatie staan op de volgende twee websites:
https://debian-handbook.info/browse/stable/sect.installation-steps.html
https://doc.opensuse.org/documentation/leap/security/html/book.security/cha.security.cryptofs.html#sec.security.cryptofs.y2.part_inst

LUKS-CONTAINERS

Als je je laptop al helemaal hebt ingericht of je er bewust voor kiest om niet alles van je laptop te