UiT Norges arktiske universitet

Retningslinje for herding av IKT-systemer

Fastsatt av:	IT-direktør	Dato:	07.11.2023
Ansvarlig enhet:	ITA BASE PRO	Id:	
Sist endret av:	Faggruppeleder BASE-PRO	Dato:	07.11.2023
Erstatter:	Ny	Arkivref.:	2023/965

Formål

Systemherding er prosessen med å sikre en server eller et datasystem ved å minimere angrepsoverflaten, eller sårbarhetsoverflaten, og potensielle angrepsvektorer. Det er en nett- og applikasjonsangrepsbeskyttelse som innebærer å lukke systemets sårbarheter som nettangripere kan bruke for å utnytte systemet og få tilgang til brukernes sensitive data.

Virkeområde

Retningslinjen gjelder for alle datasystem forvaltet av UIT, uavhengig om de driftes av ITA eller andre

Ansvar, myndighet og oppgavefordeling

IT-direktør eller den hen bemyndiger fastsetter og vedtar denne retningslinjen.
Faggruppene har ansvaret for iverksettelse, evaluering og vedlikehold av denne retningslinjen, herunder å fremme forslag om endringer til IT-direktør.

Definisjoner og forkortelser

Med datasystem menes klientmaskiner, servere, nettutstyr, AV-utstyr, IOT, låseanlegg, sd-komponenter (bygningsdrift) m.m.

Beskrivelse

Formålet skal oppnås ved at vi til enhver tid har kontroll over hvilke IT-ressurser vi har på UIT.
En del av elimineringsprosessen for systemherding involverer sletting eller deaktivering av unødvendige systemapplikasjoner, tillatelser, porter, brukerkontoer og andre funksjoner slik at angripere har færre muligheter til å få tilgang til sensitiv informasjon til et virksomhetskritisk eller kritisk infrastrukturdatasystem.

Hovedsakelig er systemherding en metode for å beskytte et system mot angrep utført av nettkriminelle. Det innebærer å sikre et datasystems programvare hovedsakelig, men også hardware og andre systemelementer for å redusere sårbarheter og en potensiell kompromittering av hele systemet.

- Installer kun de programmene og tjenestene som er nødvendige for å utføre arbeidsoppgavene, og fjern unødvendige programmer og tjenester som kan være en kilde til sårbarhet.
- Brannmur og sikkerhetsinnstillinger skal brukes for å blokkere uønsket trafikk og hindre uautorisert tilgang.
- Begrens brukerrettigheter til å kun tillate de aktivitetene som er nødvendige for å utføre arbeidsoppgavene, og unngå å gi brukere høyere rettigheter enn de trenger.

- Implementer autentisering og autorisasjonsmetoder, inkludert to-faktor autentisering, der det er mulig for å sikre at bare godkjente brukere får tilgang til systemet.
- Overvåke systemaktiviteter og lagre logger for å identifisere og reagere raskt på sikkerhetstrusler.
- Utfør regelmessige sikkerhetsskanninger og tester for å identifisere sårbarheter og feil i systemet, og ta nødvendige tiltak for å løse problemene.
- Oppdater systemet regelmessig med sikkerhetsoppdateringer og programvareoppdateringer for å tette sårbarheter og forbedre sikkerheten.
- Følge leverandør av systemet sine anbefalinger og beste praksis.
- Endre eventuelle standardpassord.

Referanser

- Prinsipper og retningslinjer for forvaltning av forskningsdata ved UiT, lenke
- Ledelsessystem for informasjonssikkerhet og personvern, Lenke
- Retningslinje for klassifisering av informasjon, Lenke