CENTER FOR CYBERSIKKERHED

Cybersikkerhed i overvågningsudstyr

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

Forsideillustration: Shutterstock/PongMoji

Indledning

For at hjælpe offentlige og private organisationer præsenterer Center for Cybersikkerhed i denne vejledning en samling konkrete anbefalinger til indkøb, opsætning, drift og bortskaffelse af overvågningsudstyr.

Målgruppen er primært de medarbejdere, der har ansvaret for at styre organisationens indkøb og drift af overvågningsudstyret. Dele af vejledningen henvender sig til ledelsen, der skal træffe de strategiske beslutninger om overvågningsudstyr.

I vejledningen anvendes ordet overvågningsudstyr om overvågningskameraet og dets firmware og software. Anbefalingerne forholder sig primært til overvågningsudstyr, men også til den netværksinfrastruktur overvågningsudstyret er forbundet til.

Overvågningsudstyr er meget anvendt både i den offentlige og private sektor. Men i udstyr, der tilkobles netværksinfrastrukturen, kan der ligge en del sårbarheder, der kan udnyttes af en trusselsaktør.

Overvågningen foretages ofte af overvågningsudstyr forbundet til internettet. Derfor er størstedelen af overvågningsudstyr kategoriseret som IoT-enheder (Internet of Things). Alle IoT-enheder kan indeholde sårbarheder. Derfor skal disse risici håndteres af organisationen. Der er i overvågningsudstyr, der er forbundet til internettet, en risiko for, at andre kan se med.

Overvågningsudstyr, som er tilkoblet internettet, giver ligeledes en sårbarhed for kompromittering af andre systemer. Overvågningsudstyr kan eksempelvis anvendes af en hacker som indgang til organisationens netværk.

Noget overvågningsudstyr kan indsamle sensitive data, der fordrer en høj beskyttelse. Det kan eksempelvis være billeder af personer, produkter eller industriprocesser. Derfor skal der gennemføres en risikovurdering baseret på anvendelsen og placeringen af overvågningsudstyret både fysisk og i it-infrastrukturen.

Hvor overvågningsudstyr og andre IoT-enheder vurderes at udgøre en uacceptabel risiko, kan en modforanstaltning være at placere det i et særligt segmenteret netværk.

Det er vanskeligt at undersøge, om overvågningsudstyr fra en bestemt producent indeholder andre end kendte sårbarheder. Derfor skal enhver organisation have retningslinjer for indkøb, opsætning og drift af overvågningsudstyret. Af retningslinjerne skal det fremgå, hvorvidt udvalgte produkter skal undgås, eller hvilke krav der skal stilles til netværkssegmentet, det er placeret i.

Ved anskaffelse af overvågningsudstyr skal organisationen være opmærksom på, at der kan opstå situationer, hvor leverandøren af overvågningsudstyr ikke har mulighed for at opgradere hard- eller software. Derved risikerer organisationen en øget sårbarhed. Denne problematik kan navnlig opstå, såfremt udstyret er omfattet af USA's Entity List beskrevet i denne vejledning.

Vejledningen forholder sig ikke til behandling af personoplysninger. Her henviser Center for Cybersikkerhed til Datatilsynets vejledning *Optagelser og overvågning*. Den beskriver grundlæggende krav til behandling af personoplysninger, behandlingsreglerne og en række andre regler, der er relevante i forbindelse med overvågning.

Overordnede anbefalinger

- Organisationen bør sikre sig, at informationssikkerheden i dens leverandørforhold er passende.
- Organisationen bør sikre, at dens software er opdateret.
- Organisationen bør sikre, at dens netværk er segmenteret.
- Organisationen bør registrere overvågningsudstyrets placering.
- Organisationen bør ændre standardpassword på overvågningsudstyr.
- Organisationen bør bortskaffe sit overvågningsudstyr på en sikker måde.

Leverandørforhold

Sikkerheden ved det udstyr, man indkøber, kan afhænge af den sikkerhed, leverandøren stiller til rådighed. For yderligere information kan man læse Vejledning om leverandørforhold (Center for Cybersikkerhed [CFCS] og Digitaliseringsstyrelsen 2022).

Ved anskaffelse af overvågningsudstyr bør organisationen være opmærksom på, om leverandøren eller produktet er omfattet af andre landes eksportkontrol, som kan medføre forhold, der har indflydelse på leverandørens mulighed for leverance, support og opdatering af produktet. Det kan for eksempel være om leverandøren er registreret på USA's Bureau of Industry and Security såkaldte *Entity List*.

Anbefaling
Organisationen bør stille krav til leverandøren om dokumentation og håndtering af sårbarheder i overvågningsudstyr.

Formål
At sikre at kendte sårbarheder håndteres, og at der stilles opdateret soft- og firmware til rådighed for kundens organisation.

Anvisning
Organisationen bør sikre, at leverandøren dokumenterer følgende:

- At leverandøren ikke har adgang til overvågningsudstyret uden organisationens vidende.
- Løbende sikkerhedstest af deres produkter.
- Sikkerhedsopdatering af produkter ved sårbarhedsrapporteringer.
- Kommunikation ved udgivelse af nye sikkerhedsopdateringer.
- Etablering af en sikker distributionsmetode for sikkerhedsopdateringerne.
- At der udgives tilstrækkelige anvisninger om installation af sikkerhedsopdateringer.
- Oprindelsesland på udstyret og indholdet i udstyret.

Det er væsentligt at undersøge, om produktet kan være fremstillet af en Original Equipment Manufacturer (OEM) og solgt under forskellige varemærker. Hvis dette er tilfældet, kan samme teknologi og eventuelle sårbarheder findes i produkterne (IPVM 2022).

Opdatering af software

Opdatering af software til overvågningsudstyret er lige så vigtigt som opdatering af andet software. Denne anbefaling omhandler, at organisationen har processer for at sikre implementering af sikkerhedsopdateringer.

Anbefaling
Overvågningsudstyret og underliggende systemer bør altid være opdateret med seneste version af softwaren.

Formål
Opdateringer af software reducerer sandsynligheden for, at hackere udnytter kendte sårbarheder i overvågningsudstyret.

Anvisning
Organisationen bør have:

- En liste over alt overvågningsudstyr i organisationen.
- Et værktøj, der understøtter automatisk installation af de af organisationen godkendte opdateringer.
- En dokumenteret proces for installation af opdateringer/patch af software, der ikke kan håndteres af ovennævnte værktøj til automatisk installation.
- En dokumenteret proces, der dækker overvågningsudstyrets og netværkskomponenters opdatering af hardware, software og firmware.

Segmentering af netværk

Med segmentering inddeler man logisk eller fysisk sit netværk i mindre dele ud fra kriterier besluttet i den overordnede informationssikkerhedspolitik. Denne anbefaling handler om at segmentere overvågningsudstyret fra resten af organisationens netværk. Dette øger organisationens resiliens for cyberangreb. Samtidig gør segmentering det lettere at monitorere og filtrere trafikken på netværket.

Anbefaling
Overvågningsudstyr bør begrænses til et dedikeret netværk og monitoreres.

Formål
Segmentering af et netværk mindsker sandsynligheder for, at et angreb kan sprede sig. Samtidig gør segmentering det lettere at monitorere og reagere på afvigelser fra i normalbilledet.

Anvisning
Organisationen bør:

- Have organisationens netværk kortlagt og dokumenteret.
- Have et separat netværk til overvågningsudstyr.
- Sikre at kun overvågningsudstyr er koblet til netværket.
- Logge og monitorere trafikken på netværket til overvågningsudstyret på flere parametre, herunder tid (UTC), konfigurationsændringer og brugeradgange (CFCS 2021b).
- Konfigurere netværket, så ikke-godkendt trafik blokeres.
- Blokere trafik til andre ikke-relevante lokale netværk.
- Sikre at enheder, som opbevarer data fra overvågningsudstyret, er isoleret på netværket til overvågning.

Er overvågningsudstyret koblet til internettet, bør det krypteres med TLS 1.2 eller TLS 1.3 (CFCS 2022c).

Anvender overvågningsudstyret en trådløs forbindelse, bør der benyttes WPA2- eller WPA3-kryptering mellem enhed og access-point.

Opsætning af overvågningsudstyr

Det er vigtigt, at opsætningen af overvågningsudstyret er dokumenteret, og at alle organisationens enheder har samme sikre konfiguration.

Anbefaling
Organisationen bør have en dokumenteret procedure for opsætning og konfiguration af overvågningsudstyr.

Formål
Overvågningsudstyrs standardkonfiguration kan i visse tilfælde udnyttes af hackerne. Gennem en opsætnings- og konfigurationsproces af overvågningsudstyret kan organisationen reducere sårbarheder.

Anvisning
Organisationen bør have dokumenteret alt overvågningsudstyr. Dette indbefatter:

- Navn og type på den enkelte enhed
- Anskaffelsesdato
- Dato for konfiguration
- IP-adressen på den enkelte enhed
- Den fysiske placering for den enkelte enhed.
- Hvem der har adgang til at konfigurere overvågningsudstyret.

Ved opsætning af overvågningsudstyr bør organisationen:

- Vælge et unikt og stærkt password, der følger organisationens passwordpolitik.
- Frakoble funktionaliteter, der ikke anvendes eksempelvis wifi, Bluetooth og usb-porte.
- Afinstallere eller deaktivere unødvendige services og applikationer.
- Indføre brugerstyring for at begrænse antallet af brugeradgange med administratorrettigheder.

Overvågningsudstyret bør kunne logge hændelser såsom ændringer i dets opsætning og brug.

Organisationen bør dokumentere, hvilke informationer overvågningsudstyret indsamler. Dette bør ske i overensstemmelse med organisationens risikovurdering.

Bortskaffelse af overvågningsudstyr

Når overvågningsudstyr skal bortskaffes eller leveres tilbage til en eventuel leverandør/udlejer, bør det sikres, at der ikke er lagret data på udstyret.
For yderlige information om bortskaffelse af medie se ISO (2022).

Anbefaling
Organisationen bør sikre, at udstyr, der indeholder lagringsmedier, er renset for al data, inden det kasseres eller leveres tilbage til en eventuel udlejer.

Formål
At organisationen ikke utilsigtet lader andre få adgang til dens overvågningsdata.

Anvisning

- Organisationen bør sikre, at al data på overvågningsudstyr, der skal bortskaffes, er slettet, inden det kasseres.
- Organisationen bør sikre sig dokumentation for, at al data bliver slettet, når udstyret leveres tilbage til leverandøren.

Referencer

Center for Cybersikkerhed. (2020) Logning - en del af et godt cyberforsvar. https://www.cfcs.dk/da/forebyggelse/vejledninger/logning/

Center for Cybersikkerhed. (2021a). Cyberforsvar der virker. https://www.cfcs.dk/da/forebyggelse/vejledninger/cyberforsvar-der-virker/

Center for Cybersikkerhed. (2021b). Logningspolitik. https://www.cfcs.dk/da/forebyggelse/nationale-anbefalinger/logningspolitik/

Center for Cybersikkerhed. (2022a). Cybersikkerhed på rejsen – organisationens ansvar. https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/cybersikkerhed-pa-rejsen-organisationen.pdf

Center for Cybersikkerhed. (2022b). Cybertruslen mod Danmark. https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/

Center for Cybersikkerhed. (2022c). Sikker brug af Transport Layer Security (TLS) https://www.cfcs.dk/da/forebyggelse/vejledninger/tls/

Center for Cybersikkerhed og Digitaliseringsstyrelsen. (2022). Cybersikkerhed i leverandørforhold. https://www.cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/

Datatilsynet. (u.å.). Tv-overvågning. https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/optagelser-og-overvaagning/tv-overvaagning

International Organization for Standardization. (2022).Information security, cybersecurity and privacy protection — Information security controls. [ISO/IEC 27002]. Control 7.14 – Secure disposal or re-use of equipment.

IPVM. (2022). Hikvision OEM Directory. https://ipvm.com/reports/hik-oems-dir

National Cyber Security Centre. (2020). Connecting your smart devices with confidence. https://www.ncsc.gov.uk/blog-post/connecting-smart-devices-with-confidence

National Cyber Security Centre. (2022). Organisational use of Enterprise Connected Devices. https://www.ncsc.gov.uk/report/organisational-use-of-enterprise-connected-devices

Yderligere information

Center for Cybersikkerhed. (2020). Password-sikkerhed.
https://www.cfcs.dk/da/forebyggelse/vejledninger/passwords/

Bureau of Industry and Security (BIS) har udsendt en liste over personer og virksomheder (Entity List), som er omfattet af amerikansk eksportkontrol. Den opdaterede liste findes her:
Bureau of Industry and Security. (2023). Supplement No. 4 to Part 744 of the Export Administration Regulations.
https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list