NIS2: KRYPTERING ER ET KRAV

Kryptering af data og to-faktor-godkendelse for adgang er normalt for de fleste – både på arbejdet og derhjemme. Ikke desto mindre stiller NIS2 krav til kryptering og kryptografi. Jesper Florin, leder af DBI's sikringsafdeling, og Henrik Helander Hansen, it-ansvarlig hos DBI, forklarer her betydningen.

Af DBI - Brand og sikring

Hvad drejer kryptering og kryptografi sig om i NIS2?

Kryptografi er en fællesbetegnelse for en vifte af teknologier, som er med til at beskytte data. Kryptering er en af de mest anvendte teknologier, hvor information bliver omdannet til en kode, som kun kan læses af dem, der har den rigtige nøgle til at dekryptere den. Det er en essentiel del af datasikkerhed, og med NIS2-direktivet bliver det nu et lovkrav, at virksomheder beskytter deres data ved at anvende kryptering.

Kryptering er allerede en integreret del af mange it-systemer. F.eks. kan e-mails blive krypteret, så ingen uvedkommende kan læse med. Og VPN-forbindelser, som mange anvender til hjemmearbejde, skaber en krypteret tunnel, som beskytter de data, der bliver overført. Kryptering er i vid udstrækning en del af hverdagen, uden at man tænker over det – f.eks. også når man kommunikerer med banker eller andre via en krypteret HTTPS-forbindelse i en browser.

Hvorfor er det en del af NIS2?

Selvom kryptering allerede findes mange steder, har det hidtil ikke været et lovkrav. Det har betydet, at nogle virksomheder ikke har prioriteret det i deres systemer, og det har gjort dem sårbare over for cyberangreb. NIS2 ændrer på det ved at stille klare krav til, hvordan virksomheder, der indgår i kritisk infrastruktur, skal beskytte deres data.

F.eks. har man i princippet kunnet bygge sin egen mailserver og lade den være åben. Og en mail, der er krypteret, når den bliver sendt afsted, er ikke krypteret hele vejen til modtageren, hvis ikke modtageren har kryptering aktivereret.

Hvordan skal virksomhederne konkret forholde sig til det?

For at opfylde kravene i NIS2 skal virksomheder sørge for, at både data, der overføres, og data, der opbevares, er beskyttet med kryptering. AES-nøglen, som er den stærkeste, vi har i dag – i hvert fald i det civile samfund – har 256 bit kryptering. Når data krypteres med den metode, bliver det ulæseligt for enhver, der ikke har den korrekte nøgle til at dekryptere dem.

En anden central del i NIS2-kravet om kryptografi er to-faktor-godkendelse. Den betyder, at brugerne skal gennem to separate trin for at få adgang til systemerne. Det kan være et password kombineret med en kode fra en app. Metoden sikrer, at selvom en hacker får fat i en brugers password, kan vedkommende ikke få adgang til systemet uden den anden faktor.

Hvad skal omfattes?

Som udgangspunkt er det virksomhedens it-infrastruktur, men hvis man har OT-infrastruktur – altså systemer, som styrer produktionsprocesser – skal de også omfattes af kryptering og it-sikkerhed i almindelighed. Disse systemer er typisk forbundet med it-infrastrukturen, men er oftest ikke lige så godt beskyttet. Og hvis de samtidig har ældre PLC-styringer, der – selvom de ikke er designet til det – er koblet til internettet, så man kan fjernovervåge og -styre et produktionsanlæg, går man fra noget krypteret til åbne protokoller. Og det medfører en risiko.

Hvad er en god fremgangsmåde?

Kryptografien bør anvendes, hvor det er praktisk muligt, men det bør ske pragmatisk, uden at den bliver en hæmsko for medarbejderne. Hvis man f.eks. bruger to-faktor-godkendelse til alt, risikerer man at gøre det så besværligt for medarbejderne at logge på, at de i stedet henter det, som de skal arbejde med, ned på et lokalt drev, som ikke er krypteret. Man ser gang på gang, at medarbejdere udfordrer sikkerhedsløsningerne, hvis det bliver for besværligt.

Desuden bør man se kritisk på sine leverandører. Hvis man f.eks. har et samarbejde, hvor man skal udveksle data via en webforbindelse, skal man ud over en evt. databehandleraftale have kryptering begge veje.

Man kan følge en kendt ISO-standard, f.eks. 27001, som har et rammeværktøj til kontrol. Men det er netop kun et værktøj og ingen 100 % garanti mod hackerangreb, for det skal også spille sammen med den daglige drift. Der er en masse procedurer og træning, som også skal være gennemført, ligesom systemerne skal vedligeholdes.

Er der faldgruber, man bør være opmærksom på?

Én faldgruppe er ikke at have tilstrækkeligt fokus på awareness-træningen – eller at den er for generisk. Man kan ikke træne folk i kryptografi, men man kan få medarbejderne til at forstå, hvordan den beskytter data, og hvad der kan ske, hvis man som medarbejder forsøger at omgå f.eks. to-faktor-godkendelse, herunder også den konsekvens, det kan få for medarbejderen i form af sanktion.

En meget stor faldgruppe er, at der bliver investeret for lidt i det løbende vedligehold af virksomhedens cybersikkerhed. Udviklingen hos dem med onde hensigter står ikke stille, og dermed risikerer man at sakke bagud på sikkerheden, hvis virksomhedens ledelse ikke vil investere i de nødvendige opdateringer. Selvom man selvfølgelig altid skal forsøge at minimere konsekvenserne af et cyberangreb, er det vigtigt, at den it-ansvarlige forklarer ledelsen, hvilken risiko den løber.