NIS2: VED DU, HVORDAN DU SKAL HÅNDTERE HÆNDELSER?

Lovforslagene i forbindelse med EU-direktivet NIS2 er blevet udsat og bliver først fremsat i Folketinget sidst på året. DBI anbefaler dog at fortsætte NIS2-arbejdet, da det er uvist, om virksomhederne får ekstra tid til at imødekomme de nye krav. DBI's sikkerhedsrådgivere Andreas P. Norstedt og Kiri-Louise Raben Ottosen forklarer her om hændelseshåndtering.

DBI
BRAND OG SIKRING

Hvad går hændelseshåndtering ud på?

Ifølge NIS-direktivet er det enhver handling og/eller procedure, der sigter mod at forebygge, detektere, analysere, begrænse eller reagere på en hændelse – og komme sig efter en hændelse. Med andre ord laver man procedurer for, hvad der skal ske før, under og efter en hændelse.

Hændelseshåndteringen skal reducere usikkerhed i en krisesituation ved at forberede medarbejdere i virksomheden. Når folk ved, hvad der potentielt kan ske, og hvad de i så fald skal gøre, kan de handle hurtigere, hvis det sker. Dermed bliver skaden minimeret.

Når vi taler cybersikkerhed, er det en bred vifte af hændelser, der som regel opstår pga. menneskelige fejl. Det er f.eks. phishing-angrebet, hvor en medarbejder klikker på linket i en mail, der ser ud til at komme fra en kendt virksomhed eller kollega. Dermed bliver der downloadet en ransomware, der kan lukke systemer ned i en periode. Det kan også være angreb i det skjulte, hvor den downloadede malware detekterer, hvad der sker i et system.

Samtidig er det vigtigt at tænke it-beredskabsplanen sammen med den ordinære beredskabsplan, herunder kontrollen af de fysiske adgangsforhold, fordi cyberhændelser i NIS2 ikke er afgrænset til digitale miljøer. Det kan nemlig også være en person, som skaffer sig fysisk adgang og ødelægger noget i et serverrum eller ændrer noget i systemet ad den vej. Nogle virksomheder holder de to beredskabsplaner adskilt, men det er vigtigt at tænke dem sammen i forbindelse med hændelseshåndtering.

Hvorfor er hændelseshåndtering en del af NIS2?

I forbindelse med cybersikkerhed, som NIS2 drejer sig om, er det vigtigt at være forberedt på at kunne håndtere hændelser. Det kan betale sig at være forberedt, fordi det minimerer følgeskader og reducerer virksomheders eventuelle nedetid. Man kan minimere ressourceforbrug af personer ved at have skrevet planer og procedurer ned på forhånd.

Hvordan skal virksomhederne helt konkret forholde sig til hændelseshåndtering?

Håndtering af en hændelse starter længe inden, den sker. Nærved-hændelser – altså hændelser, der er tæt på at ske, men ikke sker – kan være en god indikator for, hvad der kan ske. Derfor er det vigtigt løbende at registrere og evaluere alle hændelser, også nærved-hændelser, og om nødvendigt opdatere procedurerne efter dem.

Illustration af Rasmus Juul Pedersen

Hvad skal man have med i sin hændelseshåndtering?

Med udgangspunkt i det, der sker, før, under og efter en hændelse, er der fire temaer, der indgår i teorien "disaster management cycle": mitigering, forberedelse, respons og genopretning.

Før/mitigering:

Her ser man på farer og laver foranstaltninger for at undgå, reducere, tilpasse eller kontrollere en risiko, før en eventuel hændelse opstår. Foranstaltningerne kan bl.a. være risikovurdering og vurdering af aktiver, herunder:

- Trusselsvurdering: Foretag løbende trusselsvurderinger for at identificere potentielle sikkerhedshændelser.
- Sårbarhedsvurdering: Identificér og prioritér kritiske systemer og data. Start med at identificere de vigtigste systemer, netværk og data, som organisationen er afhængig af.
- Implementering af sikkerhedsforanstaltninger: Gennemfør proaktive foranstaltninger for at reducere risikoen for angreb, såsom patch management (opdateringer af sikkerhedssoftware), netværkssegmentering (adskillelse af netværk) og stærk adgangskontrol.
- Udvikling af it-beredskab: Udform en plan for, hvordan organisationen skal reagere på cyberangreb. Planen skal indeholde roller og ansvarsområder for personalet, kontakt til myndigheder og samarbejdspartnere samt en procedure for håndtering af hændelser. Det handler bl.a. om at etablere en krisestab i form af kompetente mennesker med mandat – herunder hvilke ressourcer de må anvende – til at håndtere de hændelser, der kan opstå. Krisestaben kan godt være støttet af eksterne eksperter og samarbejdspartnere.

Før/forberedelse:

- Oplysningskampagner på arbejdspladsen og awareness-træning af medarbejdere: De fleste hændelser kan ske pga. menneskelige fejl.
- Implementering af foranstaltninger: Byg videre på mitigeringen ved at implementere foranstaltninger som antivirus-software, firewalls, sikkerhedsprocedurer etc.
- Forberedelse af personer og udstyr i forhold til cybersikkerhed: Opbevaringskapacitet og alternative servermuligheder, sikkerhedskopiering af data etc.

Under/respons:

Det handler om at respondere på det bedst mulige grundlag, så man mindsker skader. Kontakt relevante myndigheder, og isolér det berørte system eller netværk for at forhindre yderligere spredning af skade. Indeksér også alle relevante oplysninger om angrebet, herunder tidspunktet for detektion, angrebstype og berørte systemer.

Efter/genopretning:

Her bliver processerne udbedret og genoprettet. Man skal lære af eventuelle fejl og genbesøge procedurer for alle tre faser: Før, Under, Efter.

Er der faldgruber, man bør være opmærksom på?

En udbredt faldgrube er, at virksomheder giver personspecifikke mandater i stedet for rollespecifikke mandater. Inden for it ser vi ofte, at få personer sidder med al viden, og det gør virksomheden sårbar, hvis de siger op eller ikke er tilgængelige den dag, hvor hændelsen sker.

En anden faldgrube er, at man ikke tænker helhedsorienteret og kun fokuserer cybersikkerheden på dele af virksomheden, f.eks. produktionen. Men hvis en virksomhed vil ændre sin it-sikkerhedskultur, skal det involvere alle medarbejdere. Det kan lige så vel være kantinekokken, som finder et virusinficeret USB-stick, der er tabt med vilje foran virksomheden, og sætter den i sin bærbare computer til varebestilling – som er en computer, der er forbundet med resten af virksomheden.

Når det er sagt, er det ikke alle, som skal forholde sig til alt i en it-beredskabsplan. Den bør være inddelt på niveauer, så folk kun skal forholde sig til det, som er relevant for dem, så de ikke skal navigere rundt i et 50 siders stort dokument.

Det er også vigtigt at huske dokumentationen. NIS2 stiller krav om proportionale foranstaltninger. Det vil sige, at man skal foretage en risikovurdering og planlægge sine foranstaltninger på den baggrund. Det er ikke givet, at den myndighed, der kontrollerer virksomheden, finder foranstaltningerne tilstrækkelige i forhold til risikoen. Men hvis virksomheden kan begrunde sine valg og fravalg, og myndigheden synes, at begrundelsen er tilstrækkelig, så har man styr på sin dokumentation.