OUCH! | Mai, 2018

SANS SECURITY AWARENESS

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

GDPR

Oversikt

Du har kanskje hørt om en ny lov kalt GDPR, eller General Data Protection Regulation, kalt EUs personvernforordning i Norge. Denne loven ble utarbeidet av EU, og i Norge er den tenkt å tre i kraft 1. juli. Den gjelder for enhver organisasjon som håndterer personlig informasjon for borgere i EU/EØS, uavhengig av hvor i verden den organisasjonen er basert. GDRP krever at organisasjoner opprettholder personvernet for enhver europeisk borger, og sørger for at deres personopplysninger er sikret. For at man skal kunne overholde GDPR må enkelte nøkkelprinsipper forstås og implementeres.

Folk har rett til privatliv. Organisasjoner må respektere folks privatliv ved å begrense mengden personlig informasjon de samler inn om dem og behandler, og ved å beskytte den informasjonen de har om dem. Kravene til personvern gjelder for all informasjon som, enten frittstående eller sammen med annen informasjon, kan brukes for å identifisere en levende individuell person som bor innenfor EU/EØS. Dette kan for eksempel være adresse, passnummer, førerkortnummer, detaljer om økonomi, biometrisk data, fagforeningsmedlemskap, medisinsk historie, posisjonsdata, eller informasjon relatert til en persons seksuelle legning, trosretning, eller politiske ståsted. Her er noen av hovedpunktene i GDPR som bør etterfølges:

Personopplysninger skal håndteres lovlig, rettferdig, og transparent.

Folk må bli fortalt hva som samles inn, og for hvilke formål.

Personopplysninger skal samles inn for spesifikke, eksplisitte og legitime formål. De skal ikke brukes for noe annet formål som er i strid med disse.

Personopplysninger skal kun beholdes og behandles så lenge det er absolutt nødvendig for det oppgitte formålet, ikke lenger.

Personopplysninger må være oppdaterte og korrekte.

Folk har rett til å få en kopi av sine data, og kan kreve at deres personopplysninger ikke lenger brukes, eller i noen tilfeller, slettes fullstendig.

Organisasjoner må implementere tilstrekkelige sikkerhetstiltak for å forhindre at personopplysninger blir ødelagt, går tapt, endres eller avsløres, som følge av uhell eller kriminalitet.

I tillegg må organisasjoner sørge for at alt personell som håndterer personopplysninger er tilstrekkelig opplært i hvordan de sikrer og beskytter slik data.

Tiltakene som er på plass for å sikre personopplysninger må gi et sikkerhetsnivå som er tilstrekkelig for informasjonens natur og grad av sensitivitet. Ettersom risikoen forbundet med slik informasjon vokser, burde også innsatsen og ressursbruken for nødvendige tiltak øke i takt med dette. Disse tiltakene burde gjennomgås jevnlig og oppdateres etter behov. God dokumentasjon for beslutningsprosesser og tiltak relatert til personvern og sikkerhet bidrar til å vise at man overholder kravene. Sist men ikke minst må organisasjoner melde avvik ved brudd på personvernet, senest 72 timer etter at de ble klar over det. Om organisasjoner ikke overholder GDPR kan det resultere i bøter på opptil 4% av organisasjonens globale inntekt, noe som gjør GDPR til en av de lovene i verden som potensielt er dyrest å bryte.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Gjesteredaktør

Brian Honan *er CEO for BH Consulting, som er et uavhengig konsulentfirma for cybersikkerhet og databeskyttelse, basert i Dublin i Irland. Brian har vært spesialrådgiver for Europols Cybercrime Centre (EC3), er grunnleggeren av Irlands første CERT, og er med i styret til flere innovative sikkerhetsselskaper. Finn Brian på* linkedin.com/in/brianhonan eller på Twitter: @brianhonan.

Ressurser

Sosial manipulering:	https://www.sans.org/u/Cb1
Å hjelpe andre med å sikre seg selv:	https://www.sans.org/u/Cb6
E-postregler:	https://www.sans.org/u/Cbg