OUCH! | Maj, 2018

SANS SECURITY AWARENESS

Det månedlige nyhedsbrev om IT-sikkerhed

GDPR - Persondataforordningen

Oversigt

Du har måske hørt om en ny lov kaldet GDPR, eller persondataforordning eller databeskyttelsesforordning. Denne lov er lavet af Den Europæiske Union og træder i kraft den 25. maj 2018. Den gælder for enhver organisation, der håndterer personlige oplysninger fra en person, der er bosiddende i EU, uanset hvor i verden denne organisation er beliggende. GDPR kræver, at organisationer opretholder privatlivets fred og sikkerhed for alle EU-personers personlige oplysninger. For at sikre overholdelse af GDPR skal nøgleprincipper forstås og implementeres.

Folk har ret til privatlivets fred. Organisationer skal respektere deres privatliv ved at begrænse, hvilke personlige data de indsamler, hvordan de processerer dem samt sørge for at beskytte disse data. Beskyttelse af privatlivets fred gælder for enhver information, som brugt enten alene eller sammen med andre oplysninger, kan identificere en person, der bor i EU. Disse oplysninger kan være adresser, pasnumre, kørekortnumre, finansielle detaljer, biometrisk information, fagforeningstilhørsforhold, medicinsk historie, lokationsdata eller information vedrørende en persons seksuelle, religiøse eller politiske orientering. Forordningen gælder for en "naturlig person", hvilket betyder en levende person. Her er nogle af de vigtigste principper for GDPR, der skal følges:

Personoplysninger skal behandles lovligt, retfærdigt og på en gennemsigtig måde.

Man skal oplyse om hvilke data, der indsamles og til hvilket formål.

Personoplysninger skal indsamles med angivne, udtrykkelige og legitime formål. De må ikke anvendes til andre ting, der er i strid med disse formål.

Personoplysninger skal kun opbevares og behandles så længe det er nødvendigt for det angivne formål og ikke længere end det.

Personoplysninger skal holdes ajour og korrekte.

Folk har ret til at modtage en kopi af deres data og kan anmode om, at deres personlige data ikke længere bruges eller i nogle tilfælde helt slettes.

Organisationer skal gennemføre passende sikkerhedsforanstaltninger til beskyttelse af personoplysninger mod utilsigtet eller ulovlig destruktion, tab, ændring eller offentliggørelse.

Endvidere skal organisationer sikre, at alle, der håndterer personoplysninger, er uddannet i, hvordan man sikrer og beskytter disse data.

Beskyttelsesforanstaltninger, der er lavet for at sikre personoplysninger, skal være på et niveau, der er passende for typen af de data der skal håndteres. Hvis risikoen forbundet med data bliver større, bør indsatsen og udgifterne til beskyttelse af dataene ligeledes vokse. Denne beskyttelse skal regelmæssigt gennemgås og opdateres efter behov. Veldokumenterede fortegnelser om beskyttelse af personlige oplysninger, sikkerhedsbeslutninger og foranstaltninger, hjælper med at vise, at man overholder kravene. Når data overføres til tredjeparter især uden for EU er organisationen juridisk forpligtet til at anvende foranstaltninger for at beskytte dataen, såsom kontrakter og review og jævnligt vurdere om den tredjepart lever op til kravene for at beskytte personlige data. Endelig skal organisationer i tilfælde af læk eller kompromittering af personoplysninger anmelde hændelsen inden for 72 timer efter at have fået kendskab til det. Organisationer, der ikke overholder GDPR, kan modtage bøder på op til 4% af deres globale indtægter, hvilket gør GDPR til et af de mest økonomisk bekostelige globale regler i verden.

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Gæsteredaktør

Brian Honan *er administrerende direktør for BH Consulting, et uafhængigt konsulentbureau indenfor IT-sikkerhed og databeskyttelse, som har base i Dublin. Brian har været særlig rådgiver for Europols Cybercrime Center (EC3), er grundlægger af Irlands første CERT og sidder med i flere advisory boards for innovative sikkerhedsvirksomheder. Find Brian på* www.linkedin.com/in/brianhonan eller Twitter @brianhonan.

Hvis du vil vide mere

Datatilsynets hjemmeside omkring GDPR:	https://www.dbreform.dk/
Datatilsynets vejledninger, etc. omkring GDPR:	https://www.datatilsynet.dk/vejledninger/vejledninger-databeskyttelsesforordningen/
GDPR teksten:	https://www.sans.org/u/Cbg
OUCH! Translations and Archives:	https://www.sans.org/u/D88