GDPR-nøglenetværksmøde

Sikkerhed

ÉN KOMMUNE – FEM UNIKKE STEDER
• FREDENSBORG • HUMLEBÆK • NIVÅ • KOKKEDAL • LANDET

Agenda

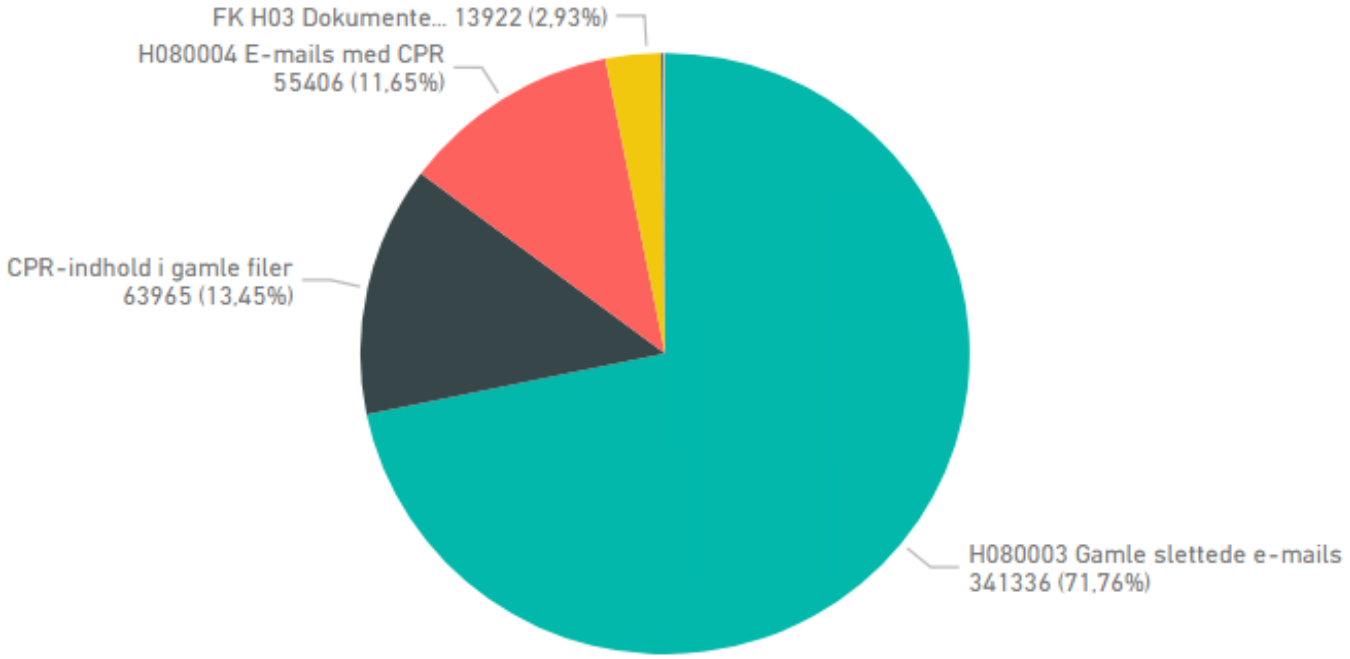
- Siden sidst
  - Slettet post i Outlook
  - System og leverandøroverblik
  - Sikkerhedsbrud (ny blanket)
- IT-sikkerhed kommer på besøg
  - Situationen i Ukraine på IT-sikkerhedsområdet
  - Smishing
  - Password politik, 12 karakterer
  - Logge på åbne netværk, risikoen ved dette

Slettet post i Outlook

Slettes automatisk: > 30 dage

Fra 1. juni 2022

Del informationen i jeres centre, hvis det ikke allerede er gjort



System og leverandøroverblik

Frist 4. april

Husk:

- Leverandører skal angives
- Fjern systemer der ikke længere er i brug
- Tilføj nye systemer
- Angiv om det er påkrævet med en databehandleraftale, og om den mangler.

	B	C	D	E	F	G
	System	**Leverandør**	**Evt: Driftes/køres hos Fredensborg eller hosted**	**Databehandleraftale påkrævet**	**Databehandleraftale mangler**	**Acadre sags nr.**
ın	Adoxa	Formpipe				18/16455
ın	Ankestyrelsens Hotlinesvar			Nej	Nej	

Sikkerhedsbrud

Ny blanket på Frede
- Dokument skal ikke længere downloades
- Kan udfyldes fra PC, tablet, mobil
- Felter er blevet obligatoriske

NB.
Indberettes som altid til GDPR-teamet hurtigst muligt.

Link til blanket:
https://fredensborg.ditmerflex.dk/fredensborg/Login/LoginAnonym?returnUrl=/fredensborg/Opret/49f198f853bf1/

FREDENSBORG KOMMUNE

Indberetning af sikkerhedsbrud i forbindelse med behandling af personoplysninger

Blanketnummer: 5979

Blanket til indberetning af sikkerhedsbrud

Vis blanketoverblik - Trin 1 af 2

Blanketten skal udfyldes hurtigst muligt efter et sikkerhedsbrud er opdaget, da der er en frist på 72 timer til at anmelde et brud til Datatilsynet.

Du bedes ikke anføre specifikke personoplysninger i skemaet. Skriv i stedet "borgeren", "personen" el.lign.

1. Kontaktoplysninger på indberetter

Fornavn *
Fornavn

Efternavn *
Efternavn

E-mailadresse *
E-mailadresse

Telefonnummer *
Telefonnummer

Center *
Indtast navn på center

2. Hændelse

Hvad er der sket? *

I dette felt skal du beskrive årsagen til hændelsen, dvs. hvorfor hændelsen er sket. Se eks. her: Hjælp

Hvor fandt hændelsen fysisk sted? *

Den fysiske adresse for en hændelse er der hvor "fejlen" sker. Hjælp

Obs. er der en mail involveret? *
- ○ Ja
- ○ Nej

Er der en databehandler/leverandør involveret? *
- ○ Ja
- ○ Nej

Hvilke personoplysninger er berørt af hændelsen? *
- ☐ Navn
- ☐ Fødselsdato
- ☐ Kontaktoplysninger
- ☐ Personnummer (cpr-nr.)
- ☐ Økonomiske forhold
- ☐ Lokationsdata
- ☐ Strafbare forhold
- ☐ Betalingsoplysninger (kreditkort mv.)

3. Tidslinje

Hvornår startede hændelsen? *
Angiv dato på formatet: dd-mm-åååå, fx. 05-02-2020

Indtast klokkeslæt

Angiv dato og klokkeslæt. Hjælp

Hvornår blev hændelsen opdaget? *
Angiv dato på formatet: dd-mm-åååå, fx. 05-02-2020

Indtast klokkeslæt

Angiv dato og klokkeslæt.

Hvordan blev hændelsen opdaget? *

Er hændelsen afsluttet? *
- ○ Ja
- ○ Nej


FREDENSBORG
KOMMUNE
IT-sikkerhed
Hvad sker der på IT-sikkerhedsområdet
ÉN KOMMUNE – FEM UNIKKE STEDER
FREDENSBORG HUMLEBÆK NIVÅ KOKKEDAL LANDET

Agenda

1. Situationen i Ukraine på IT-sikkerhedsområdet
2. Smishing.
3. Password politik, 12 karakterer
4. Logge på åbne netværk, risikoen ved dette.

Situationen i Ukraine på IT-sikkerhedsområdet

Ruslands invasion af Ukraine har fået Center for Cybersikkerhed, CFCS, til at opfordre alle myndigheder og virksomheder til at styrke deres cybersikkerhed.

Centeret forventer dog ikke, at der bliver rettet direkte destruktive cyberangreb mod Danmark, men minder om, at destruktive cyberangreb rettet mod andre lande kan sprede sig til Danmark, som man så det med Not-Petya-angrebet i 2017.

Kilde: CFCS/Version2

Links i mail

Derfor er det vigtigt at man forholder sig meget kritisk til de mail man modtager i sin indbakke.

Hvis man oplever mistænkelig mail, så har IT-sikkerhed mulighed for at oprette regel, så man ikke modtager disse. Man kan evt. vælge at blokere afsenderen og evt. domain

Her en lille video der viser hvad der kan ske, hvis man får trykket på et link: https://youtu.be/9fqnDHpKkOo

Smishing

Smishing er sammensat af begreberne "sms" (short message services") og "phishing". Når de cyberkriminelle udfører "phishing", sender de falske e-mails, der forsøger at narre modtageren til at åbne en malwareinficeret vedhæftet fil eller til at klikke på et ondsindet link. Smishing bruger simpelthen sms i stedet for e-mail.

Password politik, 12 karakterer

Husk fortsat at benytte jer af 12 karakterer eller mere når i vælger password. Store og små bogstaver, tal og evt. speciel karakterer.

Her har vi en lille video der beskriver hvordan man bedst kan huske sit password og hvad man skal være opmærksom på når man vælger et nyt password.

https://player.vimeo.com/video/461044388

Hvad er åbne netværk

Offentligt wifi, åbent offentligt netværk, gratis trådløst wifi. Det hele betyder faktisk det samme. Offentligt wifi er et netværk, som bliver stillet til rådighed af fx en cafe eller et hotel, så stedets gæster kan logge på og bruge internettet gratis. Nogle steder skal du bruge en kode, som du får udleveret, men de fleste steder klikker du bare på netværksnavnet, og så er du online.

Kilde: Stofa https://stofa.dk/blog/wifi-hotspot

Det er relativt nemt at hacke sig adgang til det data, du har på din mobil, tablet eller computer på offentlige netværk.

Vi anbefaler ikke brugen af åbne og offentlige netværk, men henviser i stedet til brugen af eget Hotspot

FREDENSBORG KOMMUNE

Tak for i dag

Bayram Polat & Jesper Reib Nielsen
IT-sikkerhed