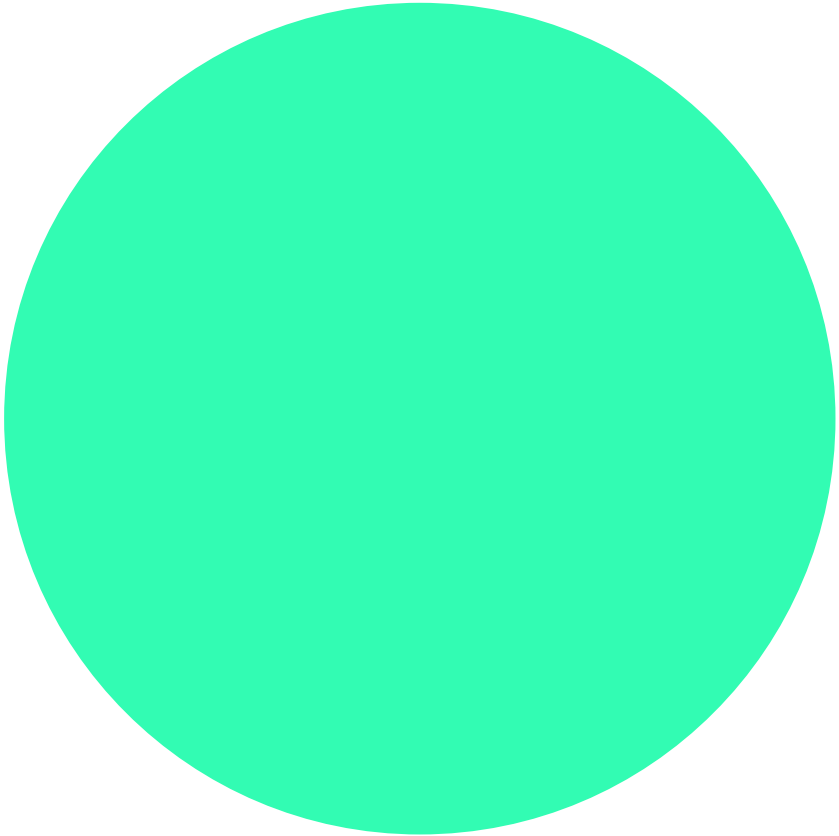
S°banken

Informasjonssikkerhet i Sbanken – utvalgte suksesskriterier



Erlend Dyrnes
Informasjonssikkerhetsansvarlig
S°banken ASA

Fakta om Sbanken

- Kjent for brukervennlige løsninger og gode betingelser
- Tilbyr også fondshandel, aksjehandel og finansiering på nett
- Norges første rene nettbank
- Åpnet i april 2000
- Landsdekkende, med kontor i Bergen
- Cirka 325 ansatte
- 380 000 aktive personkunder

★★★★★

NKB bransjevinner

I 17 år på rad har vi hatt de mest fornøyde bankkundene, i følge Norsk kundebarometer. Tusen takk for tilliten!

Vi skal gjøre det vi kan for at du skal være like fornøyd i framtiden.

Norsk Kundebarometer er et forskningsprosjekt ved Handelshøyskolen BI.

Tidligere vinnere

2016 Skandiabanken

2015 Skatteetaten

2014 Norsk Tipping

2013 Komplett.no

2012 Sparebank 1 alliansen

2011 Skandiabanken

2010 Skandiabanken

2009 Gjensidige

Fidusprisen er en pris som deles ut av NorSIS til en virksomhet som har utmerket seg med god informasjonssikkerhet. Formålet er å skjerpe bevisstheten hos privatpersoner og i virksomheter om behovet for informasjonssikkerhet.

Fakta om Erlend

- Teknisk bakgrunn
- Bred erfaring i bransjer og roller
- Ildsjel i sikkerhetsmiljøet
- Litt mer enn gjennomsnittlig interessert i
  - utøvende musikk
  - Hellas

#enkel

#vennlig rebell

Vi skal vise oss tilliten verdig

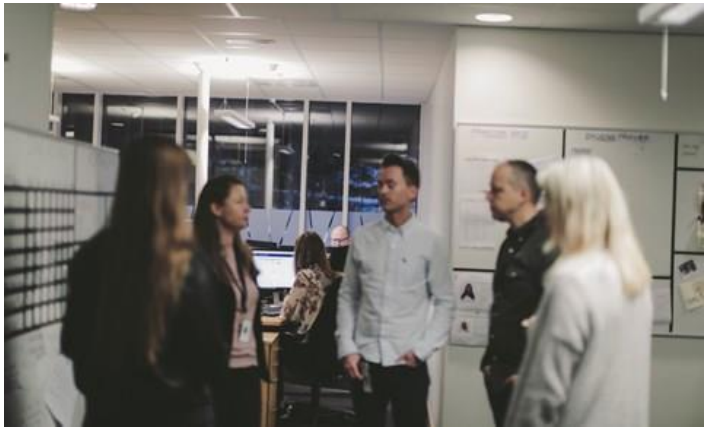
Vi skal hindre at ting går galt

Vi skal opptre i tråd med regelverket

Hva er det som treffer oss til daglig?

- Økonomisk kriminalitet
  - Svindel
  - Hvitvasking
- «Datakriminalitet»
  - Banktrojanere hos kundene
  - Avanserte dataangrep mot banken
  - Dataangrep og forsøk på sosial manipulering
- Feil i utstyr og programvare
- Hendelser hos leverandører og partnere
- Menneskelige feil hos oss og andre

… blant annet



Vi må arbeide strukturert og systematisk med informasjonssikkerhet

For Sbanken handler det om å i tilstrekkelig grad prioritere tiltak som bidrar til gode kundeopplevelser (lav sannsynlighet for at kundene våre får en negativ opplevelse)

- Målene for sikkerhetsarbeidet
- Risikovurderingene – registeret og oppfølgingen
- Dialogene med
  - Beslutningstakere
  - Leverandører
- Bevisstheten hos bankens medarbeidere

Målene må

- henge sammen med forretningens mål
- være realistiske og relevante
- være tydelige og målbare

Retningslinjer for informasjonssikkerhet i Sbanken ASA

#åpen

EKSEMPEL

Alle som jobber for Banken skal ha tilstrekkelig sikkerhetskompetanse til å forstå relevante sikkerhetskrav, vurdere hva som kan gå galt, og treffe nødvendige korrektive tiltak.

Alle som jobber for Banken skal gjennomgå relevant opplæring i informasjonssikkerhet, basert på Bankens sikkerhetskrav.

Styret og ledelsen i banken har et særskilt ansvar for informasjonssikkerhet. Det er avgjørende at oppdatert informasjon om regulatoriske forhold, relevante trusler, hendelser og svakheter, samt råd rundt effektiv eller ledende praksis gjøres tilgjengelig for dem som beslutningsunderlag.

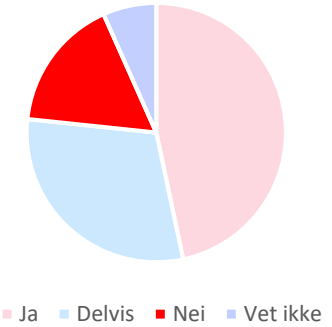
Ledere med personalansvar har ansvar for å følge medarbeidere opp rundt informasjonssikkerhet.

HR har ansvar for å tilrettelegge for opplæring i informasjonssikkerhet for nye

Målepunkter:

- Alle faste ansatte måles på gjennomføring av årlig obligatorisk e-læring
- Plan for bevisstgjøring inneholder presentasjoner og foredrag som er åpen for alle medarbeidere
- Alle avdelinger og team har årlig besøk av informasjonssikkerhetsansvarlig, personvernombud eller annen representant fra Sikkerhetsforum
- Årlige stikkprøver rundt bruk av sluttskjema viser ingen avvik

Etterlever vi våre sikkerhetskrav?



Risikovurdering

- er ikke valgfritt
- er lett å gjennomføre, og lett å få hjelp til
- er ikke komplett før man har ansvarlig og frist på tiltakene

		A	B	C	D	E
		Negligible	Minor	Moderate	Significant	Severe
E	Very Likely	Low Med	Medium	Med Hi	High	High
D	Likely	Low	Low Med	Medium	Med Hi	High
C	Possible	Low	Low Med	Medium	Med Hi	Med Hi
B	Unlikely	Low	Low Med	Low Med	Medium	Med Hi
A	Very Unlikely	Low	Low	Low Med	Medium	Medium

#enkel

EKSEMPEL

		FØR TILTAK		
Hva kan gå galt? (Risiko)	Hva gjør vi for å hindre at det går galt? (Kontroller)	Konsekvens	Sannsynlighet	Risiko
		Risikovurdering		
PC-er kan bli smittet av skadevare. Skadevaren kan gjøre felles filsystemer utilgjengelig.	Oppdatert antivirus på PC-er og gateways Bevisstgjøring Backup	Høy (4)	Mulig (3)	M

			ETTER TILTAK		
Nye tiltak	Ansvarlig	Frist	Konsekvens	Sannsynlighet	Risiko
			Risikovurdering		
Begrense antall brukere med lokale adminrettigheter Ta i bruk mer intelligent beskyttelse mot skadevare	Ole Olsen Sjef Sjefsen	Q2 2018 Q3 2018	Moderat (3)	Sjelden (2)	L

Dialogene

- er både interne og eksterne
  - med ledelsen og ansvarlige
  - med leverandørene
- må bygge på åpenhet, etterrettelighet og relevans

EKSTERN

#skvær

EKSEMPEL

INTERN

Mandat

Formål

Sbanken/Leverandør sikkerhetsforum er en møte
informasjons- og IKT-sikkerhet hos Leverandør o
gjennomgå, følge opp, diskutere og behandle sikk
temaer relevant for begge parter, samt få rapporte
sikkerhetsstatus i leveransene.

Faste møtetema

- Informasjon om håndterte eller pågående s
- Status felles handlingsplan
- Relevante oppdateringer på trusselbilde og
- Status på sikkerhetsarbeidet hos begge par
- Beredskaps- og katastrofeøvelser
- Målbilder i felles dialog og arbeid

Dokumentasjon

- Møteinnkalling med agenda
- Møtereferater (skrives av Sbanken)
- Felles risikoregister og -tiltaksplan
- Målbilder - en side med omforente mål
- Øvrig dokumentasjon tilpasses det enkelte møte

Hendelser Q1 - 2018

Kons	Ressurs	Trend	Hendelser	Påvirkning på kunden
		Ny	Hendelse i område 1	Høy
		↘	Hendelse i system A	Lav
		Ny	Hendelse i prosess Kunde	Uvesentlig
		→	Svindelforsøk mot banken	Uvesentlig
		↗	Cyberangrep mot banken	Uvesentlig
		↗	Svindelforsøk mot kunden	Moderat
		↘	Bedrageri	Lav

S˚banken

Klassifisering

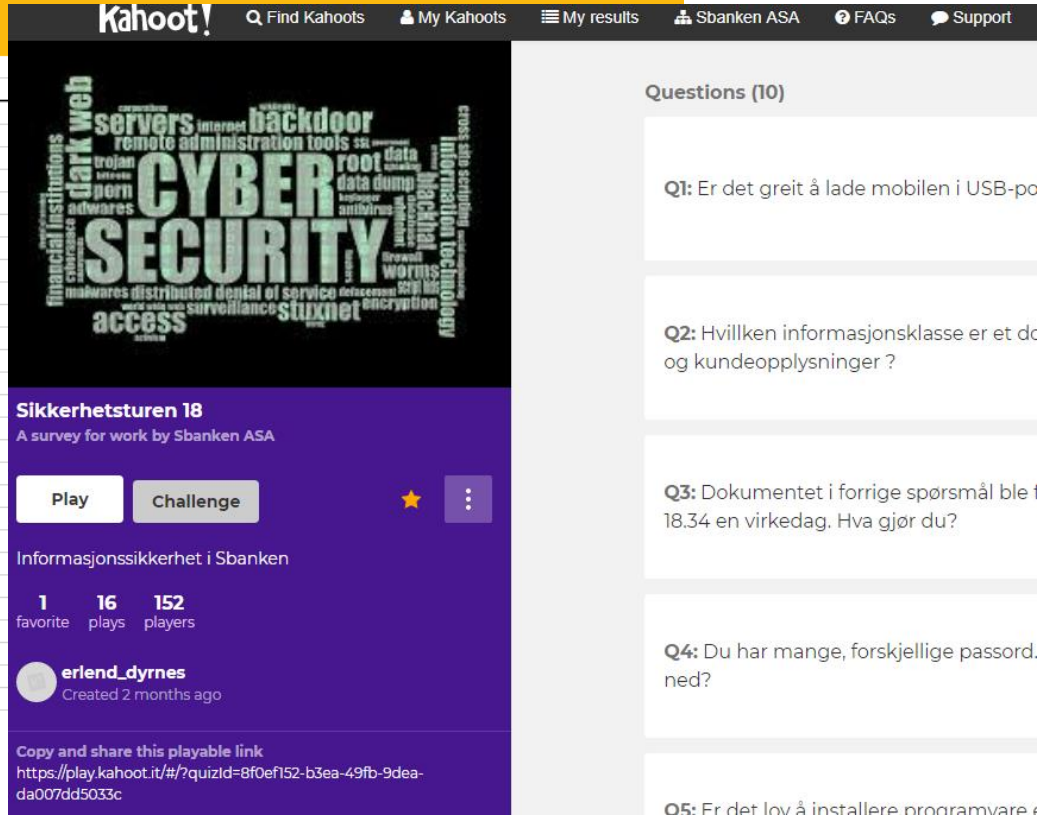
Arbeid med sikkerhetsbevisstgjøring

- må oppleves relevant og ikke påtrengende
- må bruke flere kanaler og virkemidler
- må planlegges og styres

EKSEMPEL

Informasjonssikkerhet
Interne bevisstgjøringsaktiviteter

	Dato	Aktivitet	Sikkerhetsområde
5	12.03.18	#infosec2018	Informasjonssikkerhet
6	12.03.18	#infosec2018	Informasjonssikkerhet
7	12.03.18	#infosec2018	Informasjonssikkerhet
8	13.03.18	#infosec2018	Informasjonssikkerhet
9	13.03.18	Skolebesøk	Infosec og sikker bank
0	14.03.18	Artikkel om utpressing	Utpressing
1	22.03.18	#infosec2018	Informasjonssikkerhet
2	22.03.18	#infosec2018	Informasjonssikkerhet
3	23.03.18	#infosec2018	Informasjonssikkerhet
4	05.04.18	#infosec2018	Informasjonssikkerhet
5	10.04.18	#infosec2018	Informasjonssikkerhet
6	10.04.18	#infosec2018	Informasjonssikkerhet
7	12.04.18	#infosec2018	Informasjonssikkerhet
8	12.04.18	#infosec2018	Informasjonssikkerhet
9	13.04.18	#infosec2018	Informasjonssikkerhet
0	April	Artikkel på intranett	Informasjonssikkerhet
1	17.04.18	Personvern for nyansatte på KF	Personvern
2	18.04.18	Artikkel på intranett om GDPR	Personvern
3	23.04.18	Sikkerhet for nyansatte på KS	Informasjonssikkerhet
4	27.04.18	Innlegg på Ut i skyen	Informasjonssikkerhet
5	Mai	Grunnopplæring GDPR	Personvern
6	08.05.18	Innlegg på Sikkerhet & sårbarhet	Informasjonssikkerhet
7	Mai	Spesialopplæring GDPR	Personvern
8	Juni	Nyhetsbrev	Informasjonssikkerhet
9	Juni	Sikkerhetsinfo i nettbanken	Informasjonssikkerhet
0	Juni	Artikkel på intranett	Informasjonssikkerhet
1	Juni	KOMPIS	Informasjonssikkerhet



Det skader ikke med litt humor

EKSEMPEL

Oppsummering

- Lag målbare mål, og mål etterlevelse
- Gjennomfør tiltak som er nødvendig for å ha god kontroll med risiko
- Etabler dialoger internt og eksternt – finn din form
- Jobb kontinuerlig med menneskene i organisasjonen

Takk for tiden din ☺

Still gjerne spørsmål –
jeg svarer etter beste evne

erlend.dyrnes@sbanken.no