Bodil Biering &
Henning Mortensen

Informationssikkerhed for SMV'er

- Sådan kommer du igang

Rådet for Digital Sikkerhed

CYBERJUICE

DS DANSK STANDARD

To typer motivation til at gå igang

Competitive advantage

Sleep well at night

Trend: fra konkurrencefordel til "license to operate"

Barrierer til at komme i gang hos mindre virksomheder

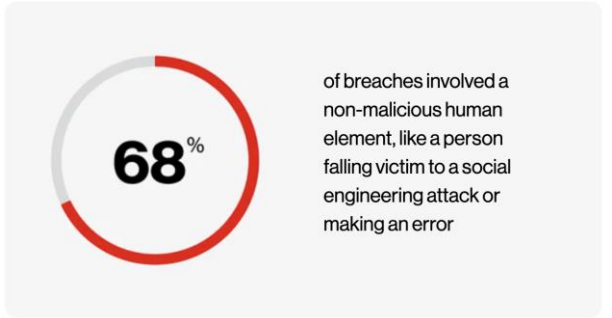
Det betaler sig at starte tidligt:

- Lille investering at implementere basics (se Hennings liste om lidt)
- Dem som starter når de er få personer kommer MEGET hurtigere igennem
- Slipper for oprydning senere
- Får det bygget ind i kulturen at sikkerhed har værdi + **gode vaner**

Menneskelige vaner vs tekniske kontroller.

👉 *Det handler ikke kun om teknologi – vaner som at genbruge svage adgangskoder, klikke på mistænkelige links eller undlade at opdatere software er ofte den reelle risiko.*

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	password	< 1 Second	4,929,113
2	123456	< 1 Second	1,523,537
3	123456789	< 1 Second	413,056
4	guest	10 Seconds	376,417
5	qwerty	< 1 Second	309,679
6	12345678	< 1 Second	284,946
7	111111	< 1 Second	229,047
8	12345	< 1 Second	188,602
9	col123456	11 Seconds	140,505
10	123123	< 1 Second	127,762



https://nordpass.com/most-common-passwords-list/

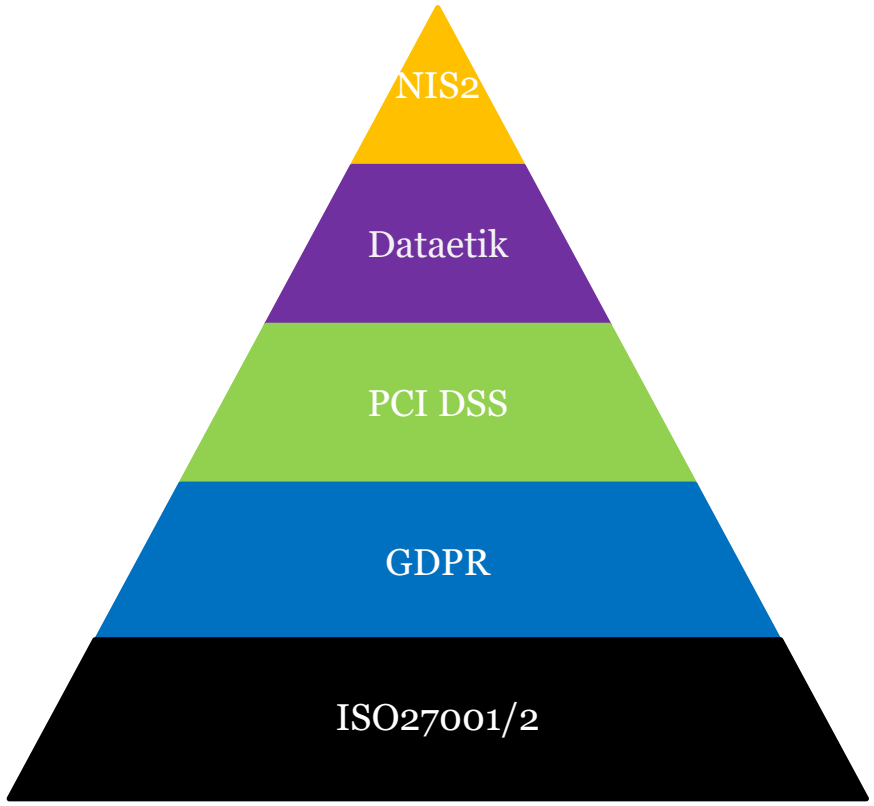
Kompleksitet

Trusler

- Udvikling i trusler
- Ny teknologi
- Ny lovgivning
- Nye krav fra samarbejdspartnere

Risici

- IT-sikkerhedsrisici
- Forretningsrisici
- Compliance risici
- Kompetencerisici



Ingen silo-dannelse

Kan man gøre det lettere?

Udspil fra Rådet for Digital Sikkerhed

- https://www.digitalsikkerhed.dk/wp-content/uploads/2024/02/202402-Vejledning-informationssikkerhed.pdf
- Kan ikke erstatte en konkret vurdering!
- Der vil ske en udbygning gennem arbejdet i Cybersikkerhedspagten.

0-10 ansatte

- Få overblik over hvilke systemer, tjenester, data og leverandører du er afhængig af
- Opdater softwareprogrammer, så sårbarheder fjernes
- Sørg for, at du har antivirus og firewall på dit udstyr
- Tag backup af data og systemer (også de data, der er i skyen) og sørg for, at den er beskyttet og udenfor virksomhedens almindelige rækkevidde (airgapped / off-line)
- Øv restore af din backup
- Lær at spotte mistænkelige mails og links
- Brug to-faktor autentifikation og hvis ikke muligt, så brug kodehusker med lange og unikke adgangskoder
- Lav en plan for hvem der gør hvad, når uheldet er ude (beredskabsplan)
- Overvej cyberforsikring

Kan man gøre det lettere?

11-50 ansatte

- Implementer de forudgående råd
- Udpeg en ansvarlig for it-sikkerhed (kan være en person, som har andre roller i forvejen)
- Sørg for medarbejderes awareness
- Sørg for at styre, hvilke brugere du har og hvilke rettigheder, de har
- Hvis du bruger fjernarbejdspladser, skal disse beskyttes med VPN, to-faktor autentifikation og kryptering af harddiske
- Sørg for en passende fysisk sikkerhed (aflåsning, afskærmning, overvågning m.v.)
- Sørg for dokumenterbar compliance med lovgivning og kundekrav (databeskyttelse, dataetik, NIS2, mv.)
- Vurder hvilke risici du står overfor og lad det være udgangspunktet for din beredskabsplan
- Test din beredskabsplan
- Hav fokus på de personoplysninger du behandler og sørg for, at de er beskyttet godt nok
- Se på din virksomhed udefra og tænk over, hvad du eksponerer, og tag stilling til om det er hensigten

Kan man gøre det lettere?

51-250 ansatte

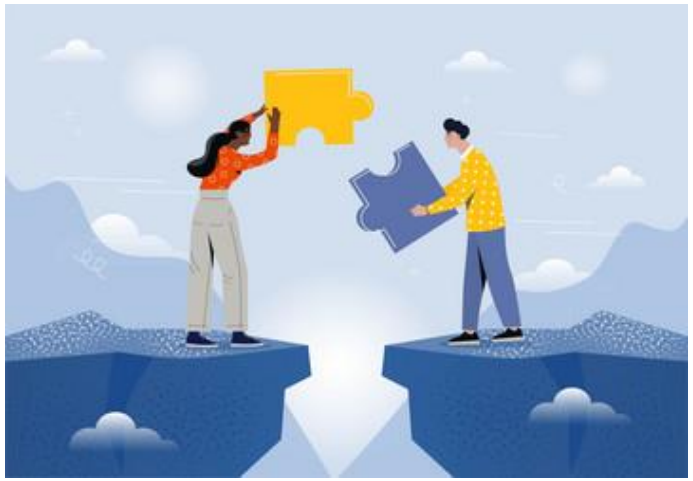
- Implementer de forudgående råd
- Sørg for at have en dokumenteret proces for risikostyring
- Skanning efter sårbarheder
- Hvis du har produktion, automatiseret lager eller tilsvarende, skal du også sørge for god beskyttelse af dette (OT). Vælg en egnet standard til dette formål.
- Netværkssegmentering
- Logopsamling og loganalyse (SIEM)
- Begræns og beskyt administrative rettigheder
- Konfigurationsstyring
- Hvis du udvikler kode, så stil krav til sikkerheden i kodeudviklingen og kontroller at kravene er opfyldt. Vælg en egnet standard til dette formål.
- Sørg for at opsamle, godkende og dokumentere ændringer på en systematisk måde.
- Sørg for at have styr på dine informationsaktiver ved anskaffelse, vedligeholdelse og bortskaffelse
- Sørg for at du har en veludviklet, opdateret og gennemtestet beredskabsplan. Planen skal være godkendt af ledelsen.
- Træn jeres medarbejdere, så de har kendskab til sikkerhedspolitikker, deres roller og ansvar
- Hændelseskommunikation til omverden, til jeres kunder og til myndighederne
- Opret en online kanal for at 3. parter kan rapportere sårbarheder på jeres produkter

Bodil Biering &
Henning Mortensen

Standarder giver mere end "bare" informationssikkerhed

80% er "bare" sund fornuft som giver orden i butikken, såsom klare roller og struktur.

Godt ledelsesværktøj til at give ramme og kommunikation omkring tekniske og organisatoriske tiltag.



Afslutning

bodil@cyberjuice.io

https://www.linkedin.com/in/bodilbiering/

&

hmo@ao.dk

https://www.linkedin.com/in/henning-mortensen-343b0/